UNITED STATES COURT OF APPEALS
FOR THE FIRST CIRCUIT

No. 23-1779

UNITED STATES,

Appellee

v.

VLADISLAV KLYUSHIN, a/k/a John Doe 1, a/k/a Vladislav Kliushin,

Defendant - Appellant

On Appeal from a Judgment of the United States District Court
for the District of Massachusetts

BRIEF OF DEFENDANT - APPELLANT VLADISLAV KLYUSHIN

Maksim Nemtsev
20 Park Plaza, Suite 1000
Boston, MA 02116
(617) 227-3700 (Telephone)
max@mnpc.law

Marc Fernich
800 Third Avenue, Floor 20
New York, NY 10022
(212) 446-2346 (Telephone)
maf@fernichlaw.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

Constitutional Provisions

Note on Citations to the Record

Material in the Addendum is cited as "Add:___."

Material in the Appendix is cited as "App:___."

"Doc.___" denotes district court docket entries.

STATEMENT

At the height of the Ukraine war, the government used the prosecution of Vladislav Klyushin, a Russian national allegedly tied to the Kremlin, as a vehicle to test drive not just one but three novel legal theories, unprecedented in the jurisprudence of the Supreme Court or this one: that stock fraud exists in the absence of a fiduciary-like duty or its breach; that the random passage of information packets through a VPN (virtual private network)[1] server otherwise unconnected to the offense conduct confers venue in any of the 94 federal judicial districts where a third-party provider chooses to place the server; and that an obscure, alternative venue statute, titled "Offenses not committed in any district" and addressing essentially foreign crimes, somehow covers essentially *domestic* offenses committed in identifiable districts within the United States – though not the one the government designated for prosecution.

[1] According to Microsoft, a VPN – a "service" available on every internet-enabled device anywhere in the world – "establishes a digital connection between your computer and a remote server owner owned by a VPN provider, creating a point-to-point tunnel that encrypts your personal data, masks your IP address, and lets you sidestep website blocks and firewalls on the internet. This ensures that your online experiences are private, protected, and more secure." https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn (retrieved Mar. 4, 2023).

None of these exercises in legal adventurism and prosecutorial overreach passes muster. This Court must reverse Klyushin's conviction.

STATEMENT OF SUBJECT MATTER AND APPELLATE JURISDICTION

This appeal arises from a judgment entered September 11, 2023, Add:1. Notice of appeal was filed a week later. App:2591. The district court had jurisdiction under 18 U.S.C. § 3231. This Court has jurisdiction under 28 U.S.C. § 1291.

QUESTIONS PRESENTED AND REVIEW STANDARDS

1. Did the district court impermissibly invade the jury's province in admitting unhelpful, untested, and unnecessary statistical opinion – coming from a partisan government economist and smacking of junk science – that purported to assert one-in-a-trillion and nine-in-a-million probabilities the stock trading patterns at issue were random, effectively directing a finding that they must have been illicit?

Evidentiary rulings are reviewed for abuse of discretion. *U.S. v. Velazquez-Fontanez*, 6 F.4th 205, 219 (CA1 2021).

2. Was venue improper, unconstitutional and in tension with the government's own manual for prosecuting computer crime where the only connection to the district of prosecution was the chance passage of information packets through third-party VPN servers that happened to be located there? And did

the district court wrongly allow testimony from a surprise witness linking the third-party servers to the district?

Questions of evidentiary sufficiency, constitutional and statutory interpretation are reviewed *de novo*. *U.S. v. Minor*, 63 F.4th 112, 117 (CA1 2023). Evidentiary rulings are reviewed for abuse of discretion. *Velazquez-Fontanez*, 6 F.4th at 219.

3. Did the trial court prejudicially err in refusing to instruct the jury that defendant had to knowingly and intentionally cause a conspiratorial act to occur in the District of Massachusetts or reasonably foresee one occurring there?

Preserved challenges to jury instructions are reviewed *de novo*. *Minor*, 63 F.4th at 117.

4. From the inception of this case – indictment and extensive pretrial motion practice – through pretrial requests to charge and eight days of trial testimony, the government insisted that venue was proper under the continuing offense statute, 18 U.S.C. § 3237, based solely on the chance passage of information packets through third-party VPN servers that happened to be in Boston. Klyushin relied on those representations and designed his defense accordingly.

After resting its case – at a charge conference on the eve of summations – the government shifted gears and floated an entirely new venue theory: that venue was also proper under 18 U.S.C. § 3238, nicknamed the "high seas" venue statute and titled "Offenses not committed in any district," because the charged offenses had begun abroad in Russia and the government had first chosen to bring Klyushin to Boston following his extradition from Switzerland.

Did the trial court improperly and unconstitutionally instruct the jury on this inapplicable and untimely alternate venue theory, violating Art. III, § 2, cl. 3 and prejudicially varying the indictment, where the charged conspiracy offense was indisputably committed in at least the districts where the corporate victims' computers were located and hacked and their stolen confidential information was traded upon – though not in the District of Massachusetts, where the government arbitrarily chose to prosecute the case?

Questions of constitutional and statutory interpretation and preserved challenges to jury instructions are reviewed *de novo*. *Minor*, 63 F.4th at 117.

5. Did the district court reversibly err in its stock fraud venue instructions by charging the jury under the general default statute for continuing offenses, 18

U.S.C. § 3237, instead of the specific statutory venue provision for stock fraud crimes?

Preserved challenges to jury instructions are reviewed *de novo*. *Id.*

6. Did the district court err in instructing the jury to find venue only by preponderant evidence rather than beyond a reasonable doubt?

Preserved challenges to jury instructions are reviewed *de novo*. *Id.*

7. The breach of a fiduciary-like duty to disclose or abstain has long been recognized as the linchpin of insider trading regulation. In this case, however, the government invented a new and novel species of stock fraud liability – unprecedented in the Supreme Court or this one – contending that misrepresenting identity online provides all the deception necessary to violate federal securities law.

Did the district court err in sustaining this duty-free approach – which would make every larceny by false pretenses that somehow touches securities a federal stock fraud offense – and instructing the jury in kind?

Questions about statutory interpretation, evidentiary sufficiency and the propriety of jury instructions are reviewed *de novo*. *Id.*

STATEMENT OF THE CASE

This appeal stems from an unprecedented prosecution in this Circuit: a hack-and-trade scheme whereby Vladislav Klyushin, a wealthy entrepreneur and the owner of a successful company, M-13, was accused of conspiring to hack Toppan Merrill ("TM") and Donnelley Financial Solutions ("DFIN"), filing agents submitting reports to the Securities and Exchange Commission ("SEC") on behalf of public companies, to obtain and trade on pre-release copies of earnings reports.

According to the government, Klyushin's Russian-based coconspirators infiltrated the computer networks of DFIN in Illinois and TM in Minnesota. These infiltrations allowed them to access unreleased earnings reports, which they purportedly used to trade in accounts belonging to Klyushin and others. Despite the government's search of Klyushin's gmail and iCloud accounts, which contained a vast amount of data, including hundreds of thousands of messages, emails, and pictures, App:2458, no evidence of the stolen releases was in any of Klyushin's electronic accounts.

Demonstrating Klyushin's involvement, the government argued, were his earnings-based trades, coinciding with the trading activities of coconspirators Igor Sladkov and Mikhail Irzak (whom Klyushin had never communicated with but who

possessed unreleased earnings reports) and bolstered by unprecedented, extraordinary statistical analyses from SEC economist Maxwell Clarke. The defense contended that Klyushin could not have orchestrated the hack, which began as early as September 2017 — 10 months before he had a trading account. The defense also maintained that Klyushin did not oversee the trading in his accounts or any accounts under his control. Rather than nonpublic information, the defense argued, Klyushin believed the trading was based on Preston, a system analyzing market sentiment developed by his company M-13, a version of which was available in Apple's app store. Additionally, the defense argued that the legal and factual grounds for venue in Massachusetts were insufficient.

Procedural Overview

In April 2021, following his March arrest in Switzerland, Klyushin was indicted on charges of conspiracy to obtain unauthorized access to computers and to commit wire and securities fraud in violation of 18 U.S.C. § 371 (Count One), wire fraud in violation of 18 U.S.C. § 1343 (Count Two), unauthorized access to a computer in violation of 18 U.S.C. 1030(a)(4) (Count Three), and securities fraud in violation of 15 U.S.C. §§ 78j(b) and 78ff(a) and 17 C.F.R.§ 240.l0b-5 (Count Four). App:34, 2446. In December 2021, Klyushin was extradited from Switzerland to

Boston. App:2446. Prior to trial, Klyushin unsuccessfully moved, *inter alia*, to dismiss Count Four. Add:6-25. A jury convicted him on all counts after a 10-day trial. App:2465. Klyushin unsuccessfully moved for acquittal at the close of the government's case and all evidence. App:1875, 2084, 2490; Doc.213. He filed a posttrial acquittal motion further addressing venue, also denied. App:2492; Add:26. The district court principally imposed a nine-year prison sentence. Add:1-5.

Trial Evidence

Evidence from TM and DFIN

Marcus Brawner of Kroll, a forensic computer expert for TM, testified that his examination of its servers revealed certain publicly available but unauthorized software that was used to "guess valid files" and "dump passwords" from users' computers. App:677, 729-31. Brawner also testified that his team reviewed unusual activity, in the form of logs spanning an approximate 90-day period (from October 14, 2019, to January 16, 2020), exhibited by certain employee accounts on TM's Bridge system hosted on servers in Minnesota, where certain client files were accessed and downloaded. App:696, 714. His review identified approximately two dozen IP addresses associated with this activity, originating, based on Microsoft logs, from Switzerland, New York, Kansas City, and other locations. App:722-24. Brawner did not locate any connections from Boston or Russia, but traced some of

the other connections back to AirVPN, a VPN provider. App:723, 732. VPN stands for "virtual private network," used commercially and privately to "create a secure connection" and provide "a measure of anonymity or privacy." App: 711, 701. Data obtained through a VPN would nonetheless go to the original user's computer. App:733. Any intruders – whom he could not identify – used Windows PC computers. App:724.

Daron Hartvigsen of StoneTurn, DFIN's forensic computer expert, similarly testified that he located unauthorized software on its networks in the United Kingdom and Poland. App:845, 793. DFIN's servers, located in Chicago, were accessible remotely from anywhere in the world through any internet connection, even a McDonalds or Starbucks. App:808. Hartvigsen identified several DFIN employees whose activities he described as suspicious and whose accounts downloaded data from DFIN's Chicago servers based on log files that extended from February 5, 2018 to August 20, 2020. App:847. The log files identified suspicious activity from 110 different IP addresses and 26 internet service providers. App:847-850. Two of the IP addresses associated with the downloads were 104.238.37.190 and 104.238.37.197. App:787-788. While some of the IP addresses were associated with VPN providers, such as AirVPN, others – including one associated with Korea

Telecommunications – weren't. App:849-50. Hartvigsen located unauthorized software, specifically PowerShell, also found on the TM network, that was modified in September 2017. App:846-47. Accordingly, he could not rule out DFIN intrusions dating that far back or even earlier. App:846-47. Hartvigsen testified that much of the unauthorized access came from a Windows computer using a Chrome browser but couldn't identify the persons responsible. App:836.

TM employee Benjamin Oliver and DFIN employees Bryan Garabo, Hyeyoung Han, Julie Soma, and Jason Lewis denied being responsible for the downloads and generally testified that they were able to login to their respective systems from anywhere in the world and only used their respective corporate VPNs. *See, e.g.*, App: 895-96, 909.

There was no evidence that Klyushin used any IP address overlapping one found on DFIN and TM's servers, including 104.238.37.190 and 104.238.37.197 – addresses allegedly hosted by a Boston-based server.[2]

[2] There was overlap between one address – 119.204.194.11 – used by Ermakov to update his iTunes account in May 2018 and located on DFIN's server during the same period attributed to a Windows computer. App:1389. There was no evidence that Ermakov was using a Windows computer at the time. There was also evidence that one of the AirVPN addresses located on TM's servers attempted to contact an M-13 server nineteen times, without a response. App:2016. There was one response later that transmitted 64 kilobytes of data, the size of approximately a

Klyushin and M-13

Klyushin owned a major Russian-based company, M-13, which provided media monitoring and cybersecurity services, including penetration testing – a common offering by cybersecurity vendors, including companies retained by TM and DFIN. App:805, 2291-92. M-13 had hundreds of employees during the relevant period and contracts with the Russian Federation and private clients. App:2291. Nikolai Rumiantcev was the company's deputy director. App:2289. In March 2020, Ivan Ermakov was listed as the company's Deputy Director General. App:2289. There was no evidence Ermakov was employed by M-13 prior to March 2020. App:1461. While M-13 employed many IT specialists, neither Ermakov nor Rumiantcev were advertised as computer experts for any of M-13's various projects. App:2289. There was no evidence that Klyushin asked anyone to hack TM, DFIN, or any other entity. Indeed, there was no evidence that Klyushin ever mentioned TM or DFIN in any of his communications. App:2455-56.

Ermakov, Sladkov, and Irzak

Klyushin met Ermakov in March 2018 when he was first added to Klyushin's phone book. App:2457. The two developed a close friendship in subsequent years.

---

small icon. App: 2016, 1999. Regardless, both Hartvigsen and defense expert J-Michael Roberts testified that IP addresses cannot be definitively attributed to a specific individual or device. App:851, 1881-82.

There was no evidence that Klyushin knew Sladkov or Irzak, who lived in St. Petersburg, some 450 miles from Klyushin's home and M-13's office in Moscow. App:1449-50. Klyushin did not have their contact information stored in his various electronic accounts, App:2455. Moreover, there was no evidence of any communication or meeting between Klyushin and these two individuals. App:1446-47.

Sladkov and his partner Olga Opukhovskaya possessed prepublication earnings reports as early as October 19, 2017. App:1456-58. Sladkov, the exclusive holder of a trading account in 2017, held additional earnings reports after October 2017. App:1456-58. Notably, images of these unreleased reports depicted Sladkov accessing them from a Windows computer—the same type used to access TM and DFIN's servers. App: 2285-86, 2437. There was no evidence that any earnings reports in Sladkov's possession or any other earnings reports were sent to or from Klyushin, Ermakov, or Rumiantcev. App:1458.

Klyushin's Trading

Klyushin opened his first trading account in July 2018 and subsequently opened accounts for M-13 and his investors. App:1459. But all trading in those accounts was carried out exclusively by Ermakov and Rumiantcev, the sole

participants in an ongoing chat discussing stock purchasing decisions and profits until May 2019. App:1473-74. That's when Klyushin and another unidentified individual were added to the conversation, but they did not contribute to trading decisions. App:1473-74. Indeed, Klyushin told chat participants that he was of no use in active trading. App:2288.

There was substantial evidence that Klyushin believed the disputed trades were based on M-13's proprietary media monitoring technology, capable of tracking some 40,000 publications at once. App:2291. Preston – an app M-13 developed as an extension of its core business – analyzed news and social media for stock market sentiment. App:1230, 1427. Preston was available in the Apple Store and previewed to Saxo Bank, which was interested in the system and impressed with its capabilities, during its relationship with Klyushin. App:2447-48. Klyushin openly told Ermakov and Rumiantcev in the chat session that he believed the trading was based on neuron networks and monitoring, *i.e.*, Preston. App:2288, 1427.

The government argued that Klyushin's trading was based on nonpublic information, relying on evidence that his earnings-based trading was much more profitable than his other trading and coincided with the trading activities of Sladkov and Irzak, who possessed unreleased earnings reports. App:2449. Specifically, the

government, through Maxwell Clarke, introduced evidence that Klyushin had traded in 356 earnings events. App:1758. Sladkov traded in 227 of the same earnings events and Irzak in 260 of the same earnings reports, *i.e.*, their trading overlapped approximately 65-75% of the time, and when trading overlapped, they traded in the same direction 97% of the time. App:2449. Further bolstering the argument were Clarke's statistical analyses positing a less than one-in-a-trillion chance that Klyushin's trading activity was random with respect to companies serviced by TM or DFIN; a less than one-in-a-trillion chance that Klyushin could have randomly predicted correct earnings surprises; and a less than nine-in-a-million chance that Klyushin's trades were made randomly after an unlawful download of a DFIN-filed earnings report. App:1781-96, 1841-55, 2426, 2423 2425.

ARGUMENT SUMMARY

1. A government economist was permitted to opine, over objection, that there were one-in-a-trillion and nine-in-a-million probabilities that the stock trading patterns at issue were random. The testimony was inadmissible junk science. It wasn't necessary, didn't help the jury and wasn't beyond their ken. Instead, it was overwhelmingly prejudicial – merely telling the jury how to vote – and should have been excluded.

2. Venue was indisputably proper in at least Illinois and Minnesota, where DFIN's and TM's respective computers were located and hacked. Instead, the government opted to prosecute in Boston, the chance location – not known to or chosen by the conspirators – of third-party VPN servers through which information packets happened to pass among the hacked computers and the conspirators in Russia. That is an insufficient and unconstitutional basis for venue – and a recipe for the forum shopping the Framers abhorred. Also, the court wrongly allowed surprise witness testimony linking the third-party servers to Boston.

3. The trial court prejudicially erred in refusing to instruct the jury that Klyushin had to knowingly and intentionally cause a conspiratorial act to occur in Massachusetts or reasonably foresee one occurring there.

4. From the case's inception – indictment and extensive pretrial motion practice – through pretrial requests to charge and eight days of trial testimony, the government insisted that venue was proper under the continuing offense statute, 18 U.S.C. § 3237, based solely on the chance passage of information packets through third-party VPN servers that happened to be in Boston. Klyushin relied on those representations and designed his defense accordingly.

After resting its case – at a charge conference on the eve of summations – the government shifted gears and floated an entirely new venue theory: that venue was also proper under 18 U.S.C. § 3238, nicknamed the "high seas" venue statute and titled "Offenses not committed in any district," because the charged offenses had begun abroad in Russia and the government had first chosen to bring Klyushin to Boston following his extradition from Switzerland.

The trial court improperly and unconstitutionally instructed the jury on this inapplicable and untimely alternate venue theory, violating Art. III, § 2, cl. 3 and prejudicially varying the indictment. That's because the charged conspiracy offense was indisputably committed in at least the districts where the corporate victims' computers were located and hacked and their stolen confidential information was traded upon – though not in the District of Massachusetts, where the government arbitrarily chose to prosecute the case.

5. The district court reversibly erred in its stock fraud venue instructions by charging the jury under the general default statute for continuing offenses, 18 U.S.C. § 3237, instead of the specific statutory venue provision for stock fraud crimes.

6. The district court erred in instructing the jury to find venue only by preponderant evidence rather than beyond a reasonable doubt.

7. The breach of a fiduciary-like duty to disclose or abstain has long been recognized as the touchstone of insider trading regulation. In this case, however, the government invented a new and novel species of stock fraud liability – unprecedented in the Supreme Court or this one – contending that misrepresenting identity online provides all the deception needed to violate federal securities law.

The district court erred in sustaining this duty-free approach – which would make every larceny by false pretenses that somehow touches securities a federal stock fraud offense – and instructing the jury in kind.

ARGUMENT

I. THE DISTRICT COURT ABUSED ITS DISCRETION IN ADMITTING STATISTICAL ANALYSES ASSERTING A ONE-IN-A-TRILLION AND NINE-IN-A-MILLION CHANCE THAT THE TRADING AT ISSUE WAS RANDOM, IMPLYING A CERTAINTY THAT IT DERIVED FROM MATERIAL NONPUBLIC INFORMATION ON TM AND DFIN'S SERVERS, UNLAWFULLY USURPING THE JURY'S FACTFINDING FUNCTION AND DIRECTING A VERDICT

A. Maxwell Clarke's Statistical Tests and Testimony

Despite persistent objections both before and during the trial, the district court allowed SEC economist Maxwell Clarke to testify and present exhibits indicating there was:

> (1) a probability of less than one-in-a-trillion that Klyushin's trading activity was random with respect to companies serviced by TM or DFIN, implying a 99.9999999% certainty that Klyushin's trades were correlated to entities serviced by TM or DFIN;[3]
>
> (2) a probability of less than one-in-a-trillion that Klyushin could have randomly predicted correct earnings surprises, implying a 99.9999999% certainty that Klyushin's decisions to buy or sell were aligned with unreleased earnings wins or losses;[4] and
>
> (3) a probability of less than nine-in-a-million[5] that Klyushin's trades were made randomly after the unlawful download of earnings reports,

[3] App:1781-96, 2426.

[4] App:1841-51, 2423, 2425.

[5] Clarke revised his figure down to nine-in-a-million following the *Daubert*

implying a 99.9991% certainty that Klyushin's trades occurred after the download of stolen earnings reports from DFIN's servers.[6]

Unsurprisingly, the government harped on Clarke's testimony during its main and rebuttal summations.[7] Despite the court's cautioning the jury that Clarke would not opine on the likelihood of any government hypothesis, his opinion implicitly conveyed near certainty that Klyushin traded TM- and DFIN-serviced stocks after an unlawful server download while accurately forecasting stock price movements based on unreleased earnings reports. Effectively, Clarke's testimony conveyed with near certainty that Klyushin traded using material nonpublic information obtained from TM and DFIN's servers.

---

hearing, where he testified that the *p*-value for Klyushin's trades was "17 in a million." App:493.

[6] App:1853-55.

[7] App:2137, 2140, 2148; App:2205 ("Well, I submit to you that Mr. Clarke's testimony is essentially unchallenged, that there's a one-in-a-trillion chance that this man would trade the way he did if there was no relationship between his trading and the identity of the filing agent, there is a one-in-a-trillion chance that he would trade long where there were earnings surprises and short there were earnings surprises on the downside, if there was no relationship between those two things. There's a few-in-a-million chance that he would trade the way he did if there was no relationship between the time of his trade and when there was a download from the DFIN servers. You've heard no serious challenge to any of that.").

This prosecutor's fallacy, propagated in Clarke's analysis and testimony, originates from application of the Fisher Exact test, a statistical method commonly used in Title VII discrimination cases to assess "statistical significance in small sample sizes." *Frappied v. Affinity Gaming Black Hawk, LLC*, 966 F.3d 1038, 1052 (10th Cir. 2020). The *p*-value, *i.e.*, the one-in-a-trillion and nine-in-a-million figures proffered at trial, "represents the likelihood that an apparent association observed in a data set is the product of random chance rather than a true relationship." *Id.* (cleaned up). Notably, the test was employed by Clarke "less than a dozen" times before and never presented to a jury in a securities fraud case.[8] Similarly, the third statistic was created using the nonparametric permutation test, which Clarke had employed only once before.[9]

[8] App:436, 473, 503.

[9] To counsel's knowledge, no published opinion has addressed the admissibility of this test in the securities fraud context. Clarke said he assisted an expert who testified to results from the test in the newswire hacking case. App:503. While the test wasn't challenged there, transcripts indicate the government's expert testified to a "statistically significant pattern where Korchevsky starts trading often shortly after the news was uploaded to the newswire computer." *United States v. Korchevsky*, No. 19-197, Dkt. 62-1, App. V. II at A-388 (2d Cir). The expert proffered nothing akin to Clarke's nine-in-a-million chance figure.

In forming his conclusions, Clarke chose specific data and excluded certain transactions and variables. For example, he focused on trading activities during the alleged conspiracy periods of January 2018 and September 2020, despite those dates not aligning with the documented evidence of intrusions (February 5, 2018 through August 20, 2020) or the actual scope of trading activities (which occurred before January 2018 and after September 2020).[10] Moreover, Clarke excluded 854 out of 2,892 transactions, deeming them unrelated to earnings,[11] along with 25% of Klyushin's earnings-based trading where the earnings report didn't correspond to a significant win or loss.[12] While acknowledging the plausibility and benefits of incorporating additional data (for example, he could have implemented variables accounting for the market sentiment Klyushin said he was trading based on), Clarke dismissed such considerations as addressing a "different question" than the government posed.[13]

[10] App:1865-66.

[11] App:513.

[12] App:480; App:531.

[13] App:445-46.

Most troubling, Clarke's statistical analysis explicitly assumed, by its terms, that the stock market and decisions to buy or sell operate as a system of random selection, akin to choosing red marbles or flipping a coin.[14] By framing the analysis in this manner, Clarke sought to determine if Klyushin's trading could have occurred purely by chance. However, this approach overlooked the fundamental reality that stock market transactions are not conducted randomly; rather, they are influenced by myriad factors, including information asymmetry, market dynamics, and personal decision-making processes. As a practical matter, he ran "a statistic to see" if Klyushin's trading "could have occurred by chance," while acknowledging that "no one selects stocks randomly and nobody makes a decision to buy or sell at random."[15] There is no doubt that a fair and efficient market encourages and rewards advantages in information gained through diligence, industry, and skill. The Supreme Court recognized over 40 years ago, in the seminal criminal case in this area, that the law does not prohibit securities transactions resulting from structural disparities in information – what Justices Blackmun and Marshall called "exploit[ing] … structural informational advantages through trading in affected

[14] App:471.

[15] App:480, 1869.

securities." *Chiarella v. United States*, 445 U.S. 222, 251 (1980) (Blackmun and Marshall, JJ., dissenting).

Equating Klyushin's trading to marble selections or coin flips, he arrived at probability figures of one-in-a-trillion and nine-in-a-million that were presented to the jury. The *p*-values Clarke propounded were not well understood by the district court, which had heard extensive arguments on the subject at a *Daubert* hearing.[16] It follows that the jury also likely struggled to grasp the significance, or lack thereof, of the statistical measures Clarke advocated. His explanation of *p*-value to the jury was hardly a model of clarity:

> Q. So now we get to what the Judge was talking about, p-value, in the far left. What is the p-value? What does that mean?
>
> A. So the question is, are these things related? Like, do you get information from one from the other? The p-value is the probability of seeing 96 percent if the population mean was 44 percent. So I think a better way to explain this might be to describe it as a probability question. So if you had a big jar of marbles –
>
> THE COURT: "P" means probability? Or no?
>
> THE WITNESS: Not quite, but, yeah.[17]

[16] App:1735, 1781.

[17] App:1788.

To make matters worse, Clarke's explanation eschewed any limitations recommended by statisticians, such as clarifying that the *p*-value does not actually prove correlation.[18] Though generally accepting this proposition, Clarke also discounted it as "statistical nonsense."[19] That these eye-popping numbers were prejudicial should come as no surprise. Even the court warned the government to be "careful what [it] wish[es] for" in seeking their admission.[20]

B. The District Court Erred in Admitting Clarke's Statistical Analyses

The district court erred in dismissing Klyushin's objections under Fed R. Evid. 401, 702, and 403. At the heart of Rule 702 is the requirement that expert testimony materially "assist the jury" in "sort[ing] out [the] contested issues" in the case. *United States v. Mehanna*, 735 F.3d 32, 67 (1st Cir. 2013). Rule 403 allows the district court to exclude even "probative evidence" if its "probative value is substantially outweighed" by the "danger" of "confusing the issues" and "misleading the jury." "Expert evidence can be both powerful and quite misleading because of

[18] App:237 ("*P*-values do not measure the probability that the studied hypothesis is true, or the probability that the data were produced by random chance alone").

[19] App:524.

[20] App:559-60.

the difficulty in evaluating it. Because of this risk, the judge in weighing possible prejudice against probative force under Rule 403 ... exercises more control over experts than over lay witnesses." *United States v. Shay*, 57 F.3d 126, 134 (1st Cir. 1995).

Clarke's constructed statistical models did not address pertinent aspects of the case. They tested neither trading during the intrusion period nor trading in its entirety. Clarke himself acknowledged that incorporating more data and variables was not only feasible but could enhance the model. But neither Clarke nor the government made any attempt to include additional data and variables, claiming they would turn the inquiry into a "different question." In essence, Clarke shaped his statistical analyses to fit the government's narrative. The subjective nature of the data and variable selection alone warranted exclusion under rules 401 and 702. *Sheehan v. Daily Racing Form, Inc.*, 104 F.3d 940, 942 (7th Cir. 1997) (Fisher Exact Test flunked *Daubert* scrutiny where expert arbitrarily omitted data).

Further, Clarke's statistical models were designed to test whether the trading could have occurred by random chance. But no one claimed Klyushin's trading was random or that the purchase and sale of stocks follows a randomized process. *Shay*, 57 F.3d at 133 n.5 (requiring "that a valid connection exist between the expert's

testimony and a disputed issue."). Klyushin asserted that his trading was based on market sentiment gleaned from the Preston system, while the government argued that it was based on stolen confidential earnings reports. Whether Klyushin traded by chance was not a question "tied to the facts of the case" or one the jury needed to resolve. *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579, 591 (1993) (expert testimony should "aid the jury in resolving a factual dispute").

Finally, the district court should have minimally excluded the one-in-a-trillion and nine-in-a-million chance figures. Rule 702's own commentary warns "forensic experts" to "avoid assertions of absolute or one hundred percent certainty—or to a reasonable degree of scientific certainty—if the methodology is subjective and thus potentially subject to error." Clarke's data and variable selection , and his decision to compare securities trading to chance were not only subjective, but his emphasizing exceedingly low *p*-values likely misled the jury by creating an impression of significance or certainty. *See* Kingsley R. Browne, *Pernicious P-Values: Statistical Proof of Not Very Much*, 42 U. Dayton L. Rev. 113, 153 (2017) ("Since the *p*-value actually provides little useful relevant information, the high risk of misleading the jury greatly exceeds its scant probative value, so it simply should not be presented to the jury.").

Stripped to its essence, Clarke's testimony offered the jury what amounts to a strawman or a red herring – one that revived the very information- advantage-as-fraud theory discredited in *Chiarella*. Correlating Klyushin's trading patterns to the likelihood of chance falsely assumed the market is a creature of chance and failed to account for the possibility that the patterns arose from factors other than insider trading. By the same token, setting up chance as an artificial comparator invited the jury to improperly infer that unless the trading patterns occurred randomly – if they did not occur by chance – then they must have been illegal or otherwise wrongful.

The figures Clarke peddled were so astronomical that they implied a near certainty Klyushin traded using material nonpublic information stolen from TM and DFIN's servers. Such interpretations of the statistical evidence amplified the prosecutor's fallacy and effectively "t[old] the jury what result to reach." *Callahan v. Wilson*, 863 F.3d 144, 154 (2d Cir. 2017). It thereby "usurp[ed]" the jury's factfinding role and "substituted the expert's judgment," contributions that are neither helpful nor probative. *Id.* Any relation between Klyushin's trading and downloads from TM and DFIN's servers are questions that should have been left to the jury. An economist's testimony was unnecessary where the lay person could determine for themselves whether a pattern exists. *United States v. Lamattina*, 889

F.2d 1191, 1194 (1st Cir.1989) (expert testimony inadmissible where jury able to determine issues "to the best possible degree"). By injecting his chance figures, Clarke invaded the jury's function and directed them to find Klyushin's trading to be based on stolen information. *United States v. Montas*, 41 F.3d 775, 784 (1st Cir. 1994) ("[e]xpert testimony on a subject that is well within the bounds of a jury's ordinary experience generally has little probative value. On the other hand, the risk of unfair prejudice is real. By appearing to put the expert's stamp of approval on the government's theory, such testimony might unduly influence the jury's own assessment of the inference ... being urged.").

C. Admission of the Foregoing Statistics Was Not Harmless.

An error is harmless "only if it is 'highly probable' that the error did not contribute to the verdict." *United States v. Kilmartin*, 944 F.3d 315, 338 (1st Cir. 2019). Whether an error was harmless depends on the "probable impact of the improper evidence upon the jury." *United States v. Fulmer*, 108 F.3d 1486, 1498 (1st Cir. 1997). Important considerations include "the centrality of the tainted material, its uniqueness, its prejudicial impact, the uses to which it was put during the trial, [and] the relative strengths of the parties' cases." *Kilmartin*, 944 F.3d at 338.

As discussed, the statistical analyses presented in this case are unique, unprecedented, and contentious, marked by one-in-a-trillion and nine-in-a-million figures that likely wielded considerable impact on the jury. *United States v. Grinage*, 390 F.3d 746, 751 (2d Cir. 2004) (testimony presented with "aura of expertise and authority" increased the risk that the jury would be swayed). For good reason, never has such a statistic been presented to a jury in a criminal securities fraud trial.

The issue at trial was whether Klyushin conspired to hack into TM and DFIN's servers and trade based on unreleased earnings reports. The defense contended that Klyushin could not have perpetrated the hacks, that Klyushin's transactions (made by Ermakov and Rumiantcev) were based on other information, including market sentiment data provided by Preston, a proprietary application developed by M-13.[21] Fortifying this argument was the fact that Klyushin never possessed an unreleased earnings report or ever mentioned TM or DFIN in the hundreds of thousands of text messages, phone logs, web searches, and pictures the government collected. The sole individuals that had earnings reports in their possession were Sladkov and Irzak, but there was no evidence that Klyushin ever obtained a report for them or even spoke to them.

[21] App:1230, 1427, 2447-48, 2288.

The government's case was circumstantial. The parties offered competing and supportable interpretations of the evidence that could point to guilt or innocence. In short, the government cannot establish the requisite "high[] probab[ility]" that admission of these staggering statistics "did not contribute to the verdict." *United States v. Garcia-Sierra*, 994 F.3d 17, 35 (1st Cir. 2021).

II. VENUE IN THE DISTRICT OF MASSACHUSETTS WAS FACTUALLY AND LEGALLY INSUFFICIENT WHERE INTERNET TRAFFIC PASSED THROUGH A SERVER IN BOSTON BY CHANCE, UNBEKNOWN TO KLYUSHIN, ANY PURPORTED COCONSPIRATORS, OR ANY MEMBER OF THE PUBLIC.

The government tried Klyushin in the District of Massachusetts on charges of conspiracy, computer intrusion, wire fraud, and securities fraud. The servers invaded were in Minnesota and Illinois. The stock transactions were executed on unspecified exchanges, but none in Massachusetts. The sole basis for laying venue there was the Boston location of a VPN server leased by Stackpath through which internet traffic was routed, unbeknown to Klyushin, any purported coconspirators, or even a member of the public. None of the essential conduct elements took place in Massachusetts. At most, the Boston server was a chance location where electronic signals passed through. Yet Klyushin was brought to Boston for prosecution and

conviction. His trial in this forum violated Article III and the Sixth Amendment and requires reversal.

Further, the district court erred in allowing Aditi Shah – a witness not appearing on the government's initial witness list and first identified more than halfway through trial – to present surprise venue testimony. The defense, relying on the government's representations in its witness and exhibit lists, crafted a strategy, examined witnesses accordingly, and represented to the jury in its opening: "[N]o one from Micfo will tell you that they took that IP [a]ddress and placed it one of their servers in Boston, Massachusetts."[22] The prejudice was obvious. Beyond discrediting before the jury defense counsel and their representations emanating from the government's own witness list, adding a new witness forced the defense to rework its theories more than halfway through trial, violating Klyushin's fundamental rights to discovery, effective counsel, and fair trial. Shah's testimony should have been excluded or a mistrial declared. The district court erred in denying both requests.

[22] App:1259

A. The Constitution Requires Prosecution in the Venue where the Crime was Committed.

As the Supreme Court recognized, "[p]roper venue in criminal proceedings was a matter of concern to the Nation's founders." *United States v. Cabrales*, 524 U.S. 1, 6 (1998). Indeed, "[t]he founding generation had a deep and abiding antipathy to letting the government arbitrarily choose a venue in criminal prosecutions." *United States v. Fortenberry*, 89 F.4th 702, 712 (9th Cir. 2023). Two separate provisions of the Constitution protect the right of a criminal defendant to be tried by a jury of his peers in the place where the crime was committed – the *locus delicti*. Article III, Section 2, provides that "[t]he trial of all crimes, except in cases of impeachment, shall be by jury; and such trial shall be held in the State where the said crimes shall have been committed." The Sixth Amendment, too, requires trial "by an impartial jury of the State and district wherein the crime shall have been committed." Underscoring the right, Federal Rule of Criminal Procedure 18 provides that "prosecution shall be had in the district in which the offense was committed."

While Congress has some authority to specify where a crime is committed for venue purposes, *see, e.g., United States v. Anderson*, 328 U.S. 699, 703 (1946), it is often silent on the issue. Where that is so, a court determines the *locus delicti* by looking to the "nature of the crime alleged and the location of the act or acts

constituting it." *Id.* A court identifies the nature of the crime by assessing "the acts of the accused that violate a statute." *Johnston v. United States*, 351 U.S. 215, 220 (1956). A court identifies those acts – that is, the "conduct that constitutes an offense" – by looking to the "essential conduct elements" of the crime and then determining where the conduct took place. *United States v. Rodriguez-Moreno*, 526 U.S. 275, 280 (1999). Other elements that do not form a part of the defendant's conduct, including "circumstance element[s]," are not considered in determining the place of the crime. *Id*. at 280 n.4.

The Supreme Court's decision in *Cabrales* illustrates the distinction between conduct and non-conduct elements. In *Cabrales*, the Court considered the appropriate venue for prosecuting the violation of money-laundering statutes that prohibit transactions in proceeds of "specified unlawful activity." 524 U.S. at 8. The Court held that venue was proper only in Florida, the state in which the financial transactions took place. *See id*. at 7-8. The location of the specified unlawful activity—drug trafficking in Missouri—was "of no moment" for venue purposes because the money-laundering statutes at issue "interdict[ed] only the financial transactions" themselves, *id*. at 7. The Court noted that the government need only prove the defendant knew she was dealing with funds derived from that unlawful

activity. *Id*. at 8. Because involvement with the drug trafficking was not a conduct element of money laundering, the Court concluded that venue was improper in Missouri. *See id*. at 7-8.

The Supreme Court's decision in *Rodriguez-Moreno* is also illustrative. At issue there was the appropriate venue for a charge of using or carrying a firearm during and in relation to a crime of violence under 18 U.S.C. § 924(c)(1). *See* 526 U.S. at 276. The defendant had possessed a firearm in Maryland, but the underlying crime of violence – a kidnapping – had continued across several states, including New Jersey. *See id*. at 277. The Court held that venue was proper in New Jersey. *See id*. at 280-81. As the Court explained, an "essential conduct element" of the crime was that the defendant "committed all the acts necessary to be subject to punishment for kidnaping," as well as that he "used a firearm." *Id*. at 280. The Court contrasted the situation before it with *Cabrales*, explaining that the requirement to show underlying unlawful activity in *Cabrales* was merely a "circumstance element" that need not involve the defendant at all. *Id*. at 280 n.4.

The Supreme Court has also instructed that where a criminal statute is ambiguous as to which elements constitute conduct elements, a court should take a restrictive approach to the statute. If Congress chose not to provide for "a choice of

trial" by specifying venue, a court should not interpret a criminal statute broadly to allow for limitless venue locations. *United States v. Johnson*, 323 U.S. 273, 276 (1944). That is so even if the broader interpretation is reasonable: "If an enactment of Congress equally permits the underlying spirit of the constitutional concern for trial in the vicinage to be respected rather than to be disrespected, construction should go in the direction of constitutional policy even though not commanded by it." *Id.*

And so, it follows that in determining "the *locus delicti* of a charged offense, the court must identify the conduct constituting the offense (the nature of the crime) and then discern the location of the commission of the criminal acts." *Rodriguez-Moreno*, 526 U.S. at 279. The inquiry begins by identifying (1) the statutory prohibition charged, (2) what acts of the accused are alleged to have been committed in violation of the prohibition, and (3) where those acts occurred. The inquiry "turns on the action by the defendant that is essential to the offense, and where that specific action took place." *Fortenberry*, 89 F.4th at 707; *see also United States v. Seward*, 967 F.3d 57, 64 (1st Cir. 2020) ("the Court in *Anderson* and *Johnston* ruled out as *locus delicti* of the crimes at issue locations in which the defendant had not engaged in any conduct that satisfied an element of the crime."). Of course, it goes without

saying that venue does not turn on "chance." *Travis v. United States*, 364 U.S. 631, 636 (1961); *United States v. Auernheimer*, 748 F.3d 525, 537 (3d Cir. 2014) ("there must be some sense of venue having been freely chosen by the defendant") .

B. The Contested Server.

There is no real dispute that Boston played nothing more than a bit part or cameo role in this case: one of a chance locale that allegedly happened to associate to an intermediate IP address assigned at random by a VPN internet provider.

VPNs, as multiple witnesses testified at trial and the court itself observed, are ubiquitous,[23] used by companies and individuals to access the internet all over the world. VPNs are a subset of internet service providers like AT&T, Comcast, and Verizon that provide individuals and companies with access to the internet.[24] VPNs assign a server and route internet traffic through that server. The IP addresses that a user obtains from a VPN provider are often shared with many others, simply because there are not enough IP addresses in the world to accommodate every individual

[23] App: 2559 ("everyone is using VPNs now, right? I mean, the court uses VPNs.").

[24] App: 851-852.

device.[25] An IP address is not the same as a phone number or social security number that is generally assigned to one user.[26] The IP addresses and hence the servers that a user or device is assigned are subject to change, at random and without notice.[27]

In total, DFIN expert Daron Hartvigsen observed 110 different IP addresses associated with 26 different ISPs connecting to DFIN's network that he attributed to intruders.[28] The intruding IP addresses identified spanned various geographical areas and ISPs, including VPN providers and standard ISPs.[29] Two of those IP addresses, 104.238.37.190 and 104.238.37.197, appearing on DFIN's server logs between October 2018 and November 2018, were leased from Web2Objects by StackPath, a business-to-business and business-to-consumer VPN provider, and assigned to its subsidiary Strong Technology LLC (Strong) as of May 18, 2018.[30] Neither Strong

[25] App:1921.

[26] App:852.

[27] App:853.

[28] App:850.

[29]App:849-50.

[30] App:1535; 1538; 1550; 2410.

nor StackPath owned the servers.[31] In this instance, StackPath purported to lease the servers from Micfo, a company that was convicted of fraud in the spring of 2019 in connection with fraudulent IP address practices.[32] Whether Micfo placed the servers in Boston was the subject of a factual dispute. There were no invoices indicating that StackPath or Strong leased the server in Boston from Micfo during the relevant period in October and November of 2018.[33] Indeed, Micfo's invoices showed that an entirely different IP Address – 104.156.206.2 – resided on that exact server in November 2018.[34] No invoice was available showing the IP address assigned to the Boston server in October 2018. Only Aditi Shah – the surprise government witness – was able to affirmatively state that she placed the relevant IP addresses on the physical server in Boston on May 30, 2018.[35]

---

[31] App:1547.

[32] App:1547.

[33] App:1553.

[34] App:2459-2463.

[35] App:1562-64.

As the government admitted, there was no evidence that Klyushin, a conspirator, or anyone else had a choice to use the Boston IP addresses.[36] The record further demonstrated that Strong did not advertise or provide a status for any Boston-based servers in September 2018 or March 2019 – the periods immediately before and shortly after the late October and early November DFIN intrusions.[37] Nor was there evidence that Klyushin or any putative coconspirator signed up for or used any services of Strong or StackPath – let alone that they selected Boston as the server location to use.[38] For all intents and purposes, Klyushin or a conspirator could have sat down in a café that provided internet through Strong and had their internet traffic, like every other person in that café, unknowingly and unintentionally routed through a server in Boston. Indeed, on these facts, even the most careful individual, actively seeking to avoid a connection to Massachusetts, would have ended up having information pass through this district. Nor did the fact that the Boston IP address associated with a VPN provider make it essential to the intrusions in this case. The

[36] App:2548-49.

[37] App:1994-95.

[38] App:1554; 2548-49.

intrusions occurred over both VPN providers and standard ISP providers.[39] In other words, intruders actively used both VPN and non-VPN internet access.

Finally, in a last-ditch effort, the government argued for the first time in its Rule 29 opposition,[40] and the district court agreed over defense objection,[41] that MNPI was "downloaded" to the Boston server. There was, however, no evidence that any MNPI was stored on the Boston servers or stored on those servers and later disseminated to coconspirators[42] The server was not controlled by coconspirators[43] It was just one point (of the likely hundreds of others) that electronic information passed through to get from the DFIN or TM servers to the computer belonging to the alleged intruder. That was the unambiguous testimony of the government's own witness, Marcus Brawner:

---

[39] App:849-50.

[40] App:2501, 2506, 2509.

[41] App:2528-33, 2567-68.

[42] Hundreds of people were likely connected to the server at the same time. None of them had control of the server or could "download" any information to it.

[43] The government also argued that the conspirators caused "StackPath as an agent" to move information. App:2554. That argument was not only waived by the government, which did not seek an instruction under 18 U.S.C. § 2(b), but also meaningless. There was no evidence that Klyushin or a coconspirator told StackPath to route traffic through the Boston IP or that they had any control over that route.

> Q. In the case of the use of a VPN, would that go to the VPN computer or all the way back to the original user?
>
> A. It would go back to the original user, whether or not they were traversing or using a VPN.[44]

In short, the use of an IP address ostensibly traced to Boston was strictly coincidental, predicated purely on chance. There was not a shred of proof that Klyushin or any coconspirator did anything – that they took any step – to actuate the use of the Boston IP address. Nor was there any evidence that the use of the Boston IP was essential offense conduct in this case.

C. Proper Venue was Not in the District of Massachusetts.

Venue issues are:

> animated in part by the danger of allowing the government to choose its forum free from any external constraints. The ever-increasing ubiquity of the Internet only amplifies this concern. As we progress technologically, we must remain mindful that cybercrimes do not happen in some metaphysical location that justifies disregarding constitutional limits on venue. People and companies still exist in identifiable places in the physical world. When people commit crimes, we have the ability and obligation to ensure that they do not stand to account for those crimes

[44] App:733. That testimony is consistent with Strong's representations regarding its servers. *See* WHAT IS A VPN? | STRONGVPN, https://strongvpn.com/what-is-vpn/ (retrieved Feb 28, 2024) ("VPN endpoint servers are the hardware used to reroute your traffic").

> in forums in which they performed no essential conduct element of the crimes charged.

Auernheimer, 748 F.3d at 541.

As the Court instructed the jury, the essential conduct elements of the crimes charged in this case "involved" Klyushin or a conspirator "misrepresenting" their "identity online ***to access*** computer systems ***to obtain*** material nonpublic information ***to trade*** on the confidential information."[45] (emphasis added). None of those essential conduct elements – accessing protected computers, obtaining confidential information, or trading on confidential information – took place in the District of Massachusetts. To be sure, the defense does not deny that "access" occurred in the districts where TM and DFIN's servers were located, that the information was "obtain[ed]" by the intruders' computer in Russia, and that "trades" were placed somewhere. But "[n]o protected computer was accessed and no data … obtained," and no trade was placed in Massachusetts. *Auernheimer,* 748 F.3d at 533-34.

[45] App:2254-46.

At most, the record shows that Boston was a mere "pass through"[46] – a site that allegedly happened to associate to an intermediate IP address assigned at random by a VPN. And, tellingly, the government offered no evidence that Klyushin or his reputed cohorts took any act to route activity through the Boston-based IP address. Far from an essential conduct element, then, any remote and attenuated connection to Massachusetts was an incidental fortuity – the epitome of a "circumstance element."

The government's own manual for prosecuting computer crime illustrates the point.[47] This case's Massachusetts IP address substantially mirrors the "pass through" Arizona router that enabled access in the DOJ Manual.[48] And a close – even cursory – "look" at the facts indicates neither that "transmission of the communications themselves constitutes the criminal offense" nor that "the path of transmission [wa]s certain."[49] Rather, since the path of transmission was "unpredictable" – passing through Boston purely by chance – it is "difficult to

[46] Add:55.

[47] Add:52-56.

[48] Add:55.

[49] *Id.*

conclude that a crime was committed in [this] district merely because packets of information happened to travel through th[is] district."[50]

The cases the district court cited to support its conclusion that venue can rest in an intermediary location are inapt.[51] In *Armour Packing Co. v. United States*, the Supreme Court upheld a conviction following a trial in the Western District of Missouri for the offense of continuous carriage by rail of the defendant's products from Kansas to New York at an illegally reduced rate. The Court concluded that "[t]his is a single continuing offense … continuously committed in each district through which the transportation is received at the prohibited rate." 209 U.S. 56, 77 (1908). Transportation, however, was "an essential element of the offense" and the essential conduct that needed to be proven. Accordingly, the offense continued, and venue was proper in every jurisdiction where the "transportation" at illegal rates took place.

In *United States v. Blecker*, the false claims statute made it unlawful to "'make[] or present[]' a false claim to any agency of the United States." 657 F.2d 629, 632 (4th Cir. 1981). The defendants "knowingly" made a submission to an

[50] *Id.*

[51] Add:42.

intermediary in the Eastern District of Virgina, who processed the claims with the government. *Id.* The delivery to the intermediary was the "last act" defendants took in presenting their false claims, hence the *locus delicti* took place in the intermediary district. *Id.* at 633.

The essential conduct here, however, was not "transportation" or the "last act" for purposes of the *locus delicti*. Nor were any packets of information intentionally submitted to this district. As this Court observed in *Seward*, the *locus delicti* cannot reside in a place where the defendant "had not engaged in any conduct that satisfied an element of the crime." 967 F.3d at 64. Thus, the chance use of a Boston IP address not caused by any act of the defendant or a coconspirator cannot substantiate venue in Massachusetts.

Accordingly, venue was improper for counts Two and Three, subject to 18 U.S.C. § 3237, since no information was accessed or obtained Boston, *i.e.*, no essential offense conduct took place there. Venue for Count Four, is appropriate "in the district wherein any act or transaction constituting the violation occurred." 15 U.S.C. § 78aa. Since no act or transaction occurred in Boston, Count Four should similarly be set aside. Venue for Count One, the conspiracy count, is appropriate where the "conspiracy was entered into or where the overt act is performed." *United*

States v. Saavedra, 223 F.3d 85, 90 (2d Cir. 2000). Use of the Boston IP server, however, did not involve an act. Rather, it was predicated entirely on chance. Regardless, "the venue potential in a conspiracy case for the prosecutor to choose from is narrowed by the substantive counts the government wishes to prosecute." *Id.* at 89. Since there was no venue for the substantive counts, Count One must similarly be set aside. *Id*.

Forcing Klyushin to defend in Massachusetts implicated squarely the "extraordinarily important" and "deep … public policy" concerns – around the "unfairness and hardship" of "haul[ing]" an accused to trial in a "distant, remote, or unfriendly forum solely at the prosecutor's whim" – that led the framers to enshrine "two" separate venue "safeguard[s]" in the Constitution. *Aurenheimer*, 748 F.3d at 540-41. By choosing to prosecute Klyushin in Boston – rather than the sites of DFIN's or TM's servers – the government heedlessly defied those safeguards and ignored the "founding generation['s]" "deep and abiding antipathy to letting the government arbitrarily choose a venue in criminal prosecutions." *Fortenberry*, 89 F.4th 712. If its counsel had it their way, the government could bring criminal charges in any of the 94 federal judicial districts where somebody happens to access one of the country's tens of thousands of "VPNs": something millions of people all

over the world do every single minute of every single day, often by automated, unwitting default, for wholly benign, completely routine and entirely legitimate purposes – without regard for hardship or fairness.[52] This Court should reject such an expansive view of venue as unconstitutional and reverse the conviction on all counts.

D. The District Court Abused its Discretion in Permitting Surprise Witness Testimony.

On February 3, more than halfway through trial, the government announced to the Court and defense its intent to present surprise venue testimony from a witness not appearing on its witness list, due back on January 23.[53] Doc.156. This declaration followed the government's producing new discovery the night before and then introducing Exhibit 267 from that discovery on highly technical matters: venue and the location of an IP address. The court admonished the government for the late

[52] App:2560; App:2561 ("you're essentially asking me to say anyplace that a VPN randomly anonymizes and hits a server anywhere, without regard to the hardship to the defendant, is enough. MR. KOSTO: When there is a wire…").

[53] Doc.156.

disclosure.[54] The very next day, the government noticed its surprise witness – Aditi Shah.[55]

The government had been investigating this case since September 2019.[56] It charged Klyushin in March 2021.[57] Four-and-half years had passed since the investigation began – and nearly 22 months since Klyushin was charged and arrested. The investigation generated millions of records. In fact, the enormous volume of discovery and its late production to the defense forced the Court to postpone the trial from October 2022 to January 2023.[58]

That venue was an issue was no surprise to the government, which had "known" from the "get-go"[59] that it was in dispute. Indeed, the parties litigated evidentiary issues dealing with the location of the Boston server more than a month before trial. The defense had contested the accuracy of the government's IP

---

[54] App: 1021-22.

[55] App:1269.

[56] App:122.

[57] Doc.1.

[58] Doc.84.

[59] App:1260, 659.

geolocation service, MaxMind.[60] In response, the government dropped its reliance on MaxMind and sought to rely on contracts and invoices.[61] The invoice trail and contract trail, however, never showed Micfo billing StackPath or Strong for a server with relevant IP addresses in Boston during October and November 2018.[62] Moreover, the defense contended that Micfo's records lacked trustworthiness because the company and its sole owner had been convicted of fraud for creating and submitting false IP addresses records.[63] Though aware of these significant issues well before trial, the government provided no notice that it had sought additional records or was attempting to locate additional witnesses.

The defense was built based on the discovery the government produced and the representations made in its witness and exhibit lists. Obviously, the defense relied on those representations in forming its strategy, examining witnesses, and promising the jury in its opening: "[N]o one from Micfo will tell you that they took

[60] App:173-74; Doc.132.

[61] App:298.

[62] App:140, 2459-63.

[63] App:1531.

that IP address and placed it on one of their servers in Boston, Massachusetts."[64] Yet the government went on to do just that, belatedly noticing a witness more than halfway through the trial to undermine the defense's preparations and trial strategy.

The prejudice was obvious. Beyond discrediting before the jury counsel and their representations emanating from the government's own witness list, adding a new witness forced the defense to rework its theories more than halfway through trial. It compromised Klyushin's fundamental rights to timely discovery, effective counsel, and a fair trial. Shah's testimony should have been excluded or a mistrial declared.[65] *See United States v. Gasparik*, 141 F. Supp. 2d 361, 366 (S.D.N.Y. 2001) (where, as here, "[l]earning of this witness mid-trial has created both unfair surprise and prejudice" – particularly "because of the statements and representations defendants made in their opening statements" – court ordered preclusion in similar circumstances); *United States v. Taylor*, 71 F. Supp. 2d 420, 421-24 (D. N.J. 1999) (same; "[h]ad [defense counsel] known that the [g]overnment would present expert testimony on the fingerprint cards, she might have changed her opening statement, a portion of her cross-examination, or adopted a different trial strategy").

[64] App:653.

[65] App:1351-54.

Though the curative instruction may have alleviated concerns about the defense's opening, it also highlighted the importance of Shah who was just "recently found."[66] Nor could the instruction dispel the prejudice attending foregone defense strategies and cross-examination topics – or missed opportunities to subpoena Cogent to determine if the IPs hosted on the Boston server switched to a different IP address, 104.156.206.2, consistent with Micfo's November 2018 invoice.[67]

III. THE COURT ERRED IN DECLINING TO INSTRUCT THE JURY THAT KLYUSHIN HAD TO INTENTIONALLY AND KNOWINGLY CAUSE A CONSPIRATORIAL ACT IN THE DISTRICT OR REASONABLY FORESEE ONE OCCURRING THERE.

Klyushin requested this jury instruction:

> Venue is proper in a district where the defendant intentionally or knowingly causes an act in furtherance of the charged offense to occur or it is foreseeable that such an act would occur.[68]

This request was based on a long line of Second Circuit cases holding that venue derives only from intentional, knowing, or foreseeable acts furthering the charged offenses. *See e.g., United States v. Svoboda*, 347 F.3d 471, 483 (2d Cir.

---

[66] App:1567.

[67] App:2461.

[68] App:1699.

2003); *United States v. Bezmalinovic*, 962 F. Supp. 435, 438 (S.D.N.Y. 1997) ("purely ministerial acts" insufficient to confer venue); *United States v. Beech-Nut Nutrition Corp.*, 871 F.2d 1181, 1190 (2d Cir. 1989) ("prior and preparatory" calls and mailings into district insufficient); *United States v. Geibel*, 369 F.3d 682, 697 (2d Cir. 2004) ("anterior and remote" actions insufficient); *United States v. Tzolov*, 642 F.3d 314, 318 (2d Cir. 2011) ("going to Kennedy airport and boarding flights to meetings with investors were not a constitutive part of the substantive securities offense with which [defendant] was charged").

While agreeing that the requested instruction "might be relevant" to the facts of this case, the district court declined to give it because there was "no First Circuit law directly on point."[69] Instead, the court gave an omnibus instruction allowing a venue finding if the district had "a meaningful connection to the allegations."[70]

As discussed, it is the defendant's "actions," not "chance," that determine the appropriate, constitutionally permissible venue for trial. The withheld instruction would have spelled out those constitutional protections for the jury. The instruction

[69] App:1921-22.

[70] Add:49.

was not inconsistent with substantive law or incorporated elsewhere in the venue charge as rendered.

If anything, a foreseeability requirement is vital in the internet age. The requirement rationalizes and tempers the Second Circuit's otherwise expansive view of venue, adopted by both the district court and the government,[71] harmonizing it with precedents like *Auernheimer* and addressing the notice and process concerns raised in the DOJ Manual scenario where the path of electronic signals is neither known nor predictable. If a court is to endorse the Second Circuit's broad conception of venue, fairness dictates that it also import the same court's foreseeability requirement to properly cabin that approach's otherwise limitless reach.

The requested instruction was also "integral to an important point in the case." *United States v. Adams*, 740 F.3d 40, 45 (1st Cir. 2014). Venue was central to Klyushin's defense, counsel soundly contending there was no factual or legal basis for prosecution in Boston.

[71] Notably, the district court relied on Second Circuit precedent in its decision to uphold venue in Massachusetts, as did the government in urging its venue positions. Add:47; App:2515. All those cases required the government to prove not only a "meaningful connection" to the prosecuting district, but also that intentional, knowing, or foreseeable acts occurred there.

IV. THE DISTRICT COURT ERRED IN INSTRUCTING THE JURY ON AN ALTERNATE VENUE THEORY – UNCONSTITUTIONAL AS APPLIED IN THIS CASE – AS TO THE COUNT ONE CONSPIRACY, PREJUDICIALLY VARYING THE INDICTMENT AND REQUIRING THAT CONVICTION'S REVERSAL

After resting its case, at a charge conference on the eve of summations, the government – realizing it had blundered in prosecuting Klyushin in Boston – ambushed the defense with an entirely new and highly obscure venue theory.

Having insisted in the indictment, during extensive pretrial motion practice, and through eight trial days that essential offense conduct had somehow occurred in Beantown, the government thus made a sharp U-turn, basically telling the judge and Klyushin, "Never mind. Forget all that. It was just window dressing."

Instead, the government sprung a novel, eleventh hour assertion: that the case was properly before the court under 18 USC § 3238, a rarely used and sparsely litigated statute nicknamed the "high seas" venue act.[72]

[72] Section 3238, tellingly titled "Offenses not committed in any district," says as relevant here: "The trial of all offenses begun or committed upon the high seas, or elsewhere out of the jurisdiction of any particular State or district, shall be in the district in which the offender … is arrested or … first brought."

Judge Saris rebuffed the government's abrupt about-face as to the indictment's substantive charges – counts Two through Four – but incongruously allowed it as to the Count One conspiracy, instructing the jury accordingly.[73]

That was error. Section 3238 does not – and cannot constitutionally – apply to the conduct charged in Count One. And its last-minute application here prejudicially varied the indictment. Klyushin's conspiracy conviction must be reversed.[74]

A. The High Seas Venue Charge was Impermissible and Unconstitutional in the Circumstances Presented

No "mere formality" or "pedantic, justice-defeating technicality," questions of venue in criminal cases, to reiterate, "raise deep issues of public policy" bearing on "the fair administration of criminal justice and public confidence in it."[75] More

---

[73] Add:50-51.

[74] Where, as here, "multiple crimes are charged in a single indictment," it bears preliminary emphasis that "venue must be laid in a district where all the counts may be tried." *U.S. v. Royer*, 549 F.3d 886, 893-94 (CA2 2008). And so, since counts Two through Four couldn't be tried in Boston, neither could Count One. *See Saavedra*, 223 F.3d at 89 (noting that "the venue potential in a conspiracy case for the prosecutor to choose from is narrowed by the substantive counts the government wishes to prosecute"). The conspiracy conviction fails on this ground alone. *See* App:1945 (preserving that point).

[75] *U.S. v. Winship*, 724 F.2d 1116, 1123-24 (CA5 1984).

than "procedural" obstacles, that is, venue restrictions have "constitutional and public policy dimensions."[76]

"There is no question," the Supreme Court recently reminded, that the "vicinage right" – the ancient rule that "all causes shall be tried in the county, and by the neighborhood of the place, where the fact is committed" – was "highly prized by the founding generation," which "wielded it as a political argument of the Revolution."[77]

Indeed, the "proper place of colonial trials" – a vital "protection for the defendant" – was "so important" to the Framers that it is not only "listed as a

[76] *U.S. v. Eziyi*, No. 2:22-cr-00160-JNP-2, 2023 WL 6318118, at *1 (D. Utah Sep. 28, 2023).

[77] *Smith v. U.S.*, 599 U.S. 236, 246-448 & n.6 (2023).

grievance in the Declaration of Independence,"[78] but "safeguard[ed]"[79] twice in the Constitution[80] and "reinforced"[81] by a federal criminal rule.[82]

And the key concern "animat[ing]" these several provisions – the "danger of allowing the government to choose its forum free from any external constraints" – is "only amplifie[d]" by the "ever-increasing ubiquity of the Internet."[83]

Chief among the vicinage right's constitutional guardrails, and the one most salient here, is the Venue Clause. That provision commands, in pertinent part, that "all criminal trials … 'shall be held in the State where the said Crimes shall have been committed; but *when not committed within any State*, the Trial shall be at such Place or Places as the Congress may by Law have directed.'"[84]

---

[78] *Auernheimer*, 748 F.3d at 540; *accord Saavedra*, 223 F.3d at 92 (describing "venue requirement" as "principally a protection for the defendant").

[79] *Cabrales*, 524 U.S. at 6.

[80] *See* U.S. Const. Art. III, § 2, cl. 3 (the Venue Clause); *id.* amend. VI (the Vicinage Clause).

[81] *U.S. v. Miller*, 808 F.3d 607, 613-14 & n.5 (CA2 2015).

[82] *See* Fed. R. Crim. P. 18.

[83] *Auernheimer*, 748 F.3d at 541.

[84] *Chandler v. U.S.*, 171 F.2d 921, 931 (CA1 1948) (emphasis supplied)

By its plain terms, the Venue Clause thus decrees that a criminal defendant *must* be prosecuted in the state where the crime was committed *unless* not committed within any state.[85] Congress may *only* direct a different place for trial *if* the crime was not committed within any state. It may *not* do so otherwise.

Put differently, "Congress has broad latitude to define the locality of a crime," but *only* "[w]here the Constitution does not mandate venue in a particular district."[86] "Congress's venue statutes do not apply when the Constitution settles the issue."[87]

Here, the Venue Clause expressly mandates trial in the state and district where the Count One conspiracy was committed – unless it was not committed in any state or district. And it's beyond debate that the conspiracy *was* committed in multiple

---

(footnote omitted).

[85] "Under federal law, if a crime is committed in a judicial district, it is also committed in a state. *See* 28 U.S.C. §§ 81–131 (defining judicial districts as comprising all or part of a state, with few exceptions)." *U.S. v. Lozoya*, 982 F.3d 648, 659 n.4 (CA9 2020) (en banc) (Ikuta, Collins and Lee, JJ., concurring and dissenting).

[86] *Ibid.* at 653 n.6 (maj. op.).

[87] *Ibid.* at 652 n.4.

American states and districts, though not in Massachusetts. Because the Constitution – particularly the Venue Clause – "settles the issue," § 3738 "do[es] not apply."[88]

To explain, it's fundamental that the "offense" in a "conspiracy prosecution[]" is "*not* the initial act of agreement."[89] Rather, as Justice Scalia aptly observed, it is the "banding-together against the law effected by that act."[90] And so, it's equally "well-established" that a conspiracy continues "until its aim has been achieved,"[91] and is properly venued "in any district where" its underlying object offense "occurred."[92]

To determine where the underlying object offense occurred, Judge Saris rightly told the jury, one must "identify" its "essential conduct elements."[93]

---

[88] *Ibid.* at 652 n.4, 653 n.6.

[89] *Smith v. U.S.*, 568 U.S. 106, 113 (2013) (emphasis supplied).

[90] *Ibid.*

[91] *U.S. v. Salmonese*, 352 F.3d 608, 615 (CA2 2003); *accord, e.g., U.S. v. LaSpina*, 299 F.3d 165, 175 (CA2 2002) ("Where the object of a conspiracy is economic, the conspiracy generally continues until the conspirators receive their anticipated economic benefits.").

[92] *Auernheimer*, 748 F.3d at 533.

[93] App: 2253.

Significantly, "essential conduct elements" are not the same as the elements making up the offense and essential to proving it; they are different and substantially narrower.[94] Among other distinctions, they are "informed by where physical *conduct* occurred, not where criminal intent was formed."[95] And perhaps most "dispositive,"[96] they are defined by the "nature of the conduct" the government identifies "[i]n the indictment and at trial."[97]

Here, the government identified the essential object of the Count One conspiracy as "involv[ing]" Klyushin or a confederate "misrepresenting" their "identity online to access computer systems to obtain material nonpublic information to trade on the confidential information."[98] And the district court so instructed the jury – over objection – at the government's request.[99]

---

[94] *See Auernheimer*, 748 F.3d at 533, 534 n.4; *Miller*, 808 F.3d at 615-16.

[95] *Miller*, 808 F.3d at 615.

[96] *Ibid.* 615-16.

[97] *Auernheimer*, 748 F.3d at 533.

[98] App:2246-47

[99] *Ibid.*

There is no doubt that activity occurred in at least the states where filing agent computers housing confidential information were located and hacked – Illinois (DFIN) and Minnesota (TM) – and perhaps also in those where corresponding stock trades were executed (presumably New York). Because essential conspiratorial conduct was "committed" in identifiable states and districts, the Venue Clause *required* the crime's prosecution in one of them. The Constitution "settles the issue," so § 3738 "do[es] not apply."[100] Congress simply has no power to "direct[]" any other place for trial.

That § 3738 purportedly covers "essentially foreign" crimes, as the district court supposed,[101] does not – and cannot constitutionally – alter this conclusion. In § 3738, this Court recognized long ago, Congress merely exercised its constitutionally reserved "power of directing by law the place of trial of crimes 'not committed within any State.'"[102] Envisioned as "coextensive with the Venue

[100] *Lozoya*, 982 F.3d at 652 n.4.

[101] Add:44.

[102] *Chandler*, 171 F.2d at 931.

Clause,"[103] the statute was "meant to … appl[y] to those cases where 'there is no court which has particular cognizance of the crime.'"[104]

More precisely, § 3738 was designed to "mirror[]" and "implement the Venue Clause's exception for crimes not committed within any State," prescribing "where a crime shall be tried" in that circumstance alone.[105] It does not – and cannot – otherwise displace "constitutional requirements that crimes be tried in the state and district where they were committed."[106] Indeed, the statute's title[107] – "Offenses not

---

[103] *Lozoya*, 982 F.3d at 662 (Ikuta, Collins and Lee, JJ., concurring and dissenting).

[104] *Chandler*, 171 F.3d at 931.

[105] *Lozoya*, 982 F.3d at 660-61, 663 (concurring and dissenting op.).

[106] *Ibid.* 665.

[107] *See, e.g.*, *Dubin v. U.S.*, 599 U.S. 110, 120-21 (2023) (reaffirming that "the title of a statute and the heading of a section" are useful tools in statutory construction); *Seward*, 967 F.3d at 69-70 & n.13 (Lipez, J., dissenting) (describing "headings and titles" as "valuable" interpretive "tools," appropriately consulted in discerning "the core conduct criminalized by the statute for purposes of ascertaining venue"); *U.S. v. Pendleton*, 658 F.3d 299, 304-05 (CA3 2011) (consulting § 3238's title in construing statute).

committed in any district" – pointedly confirms what its "[l]egislative history" indicates: "§ 3238 was intended to cover extraterritorial crimes."[108]

The conspiracy charged in Count One is *not* an extraterritorial crime. To the contrary, it targeted *American* computers, *American* companies and the *American* stock market, aiming to hack the first, rob the second and game the third. And in pursuit of those goals, the conspirators, as alleged, performed key acts in readily identifiable *American* states and districts. At a minimum, they illicitly breached DFIN's computers in Illinois and TM's in Minnesota, fraudulently trading on the information they thereby stole via the New York Stock Exchange. If anything, the district court thus got it precisely backwards. The conspiracy was essentially *domestic* – *not* foreign – in conduct and character alike.

A thoughtful federal opinion from Virginia cogently illustrates the point. "[B]y its own terms," the court verified there, § 3238 is "inapplicable" – and does not confer venue – where, as here, the defendant commits "essential conduct constituting the offense within the United States."[109] It makes no difference that a

---

[108] *Lozoya*, 982 F.3d at 655, 656 n.12 (maj. op.).

[109] *U.S. v. Mallory*, 337 F. Supp. 3d 621, 632-33 (E.D. Va. 2018), *aff'd*, 40 F.4th 166 (CA4 2022), *cert. denied*, 143 S. Ct. 1088 (2023).

charged crime is a continuing offense "occurr[ing] not just" in America "but also" abroad.[110] For "when a criminal offense does not include a specific venue provision," venue "must be determined from the nature of the crime alleged and the location of the [essential] act or acts constituting it."[111] And again, the essential acts constituting the Count One conspiracy involved "misrepresent[ing …] identity online to access computer systems to obtain material nonpublic information to trade on the confidential information."[112]

It follows that the "relevant location[s] for purposes of venue in this case"[113] are minimally those domestic ones where DFIN's and TM's computers were allegedly accessed and their confidential information was thereby obtained and subsequently traded on. "Because there is no evidence" that Klyushin committed those "proscribed act[s] upon the high seas or outside of the jurisdiction of any State, venue is not established in the place of [his] arrest under § 3238."[114]

---

[110] *Ibid.* 633.

[111] *Ibid.* 632-33.

[112] App:2246-47.

[113] *Mallory*, 337 F. Supp. 3d at 633.

[114] *Ibid.*

Notably, *Mallory* distinguished the leading cases approving the statute's application to crimes occurring both here and abroad, saying they "do not hold to the contrary or compel a different result."[115] For the domestic conduct involved in those cases, unlike Klyushin's, was insubstantial, tangential and only tenuously connected to the respective conspiracies at issue – *not* essential. As the court explained at length:

> In *U.S. v. Kampiles,* the Seventh Circuit concluded that venue was proper in the district where the defendant was arrested on charges of delivering top secret material to a Soviet agent. 609 F.2d 1233 (CA7 1979). Importantly, the evidence in that case demonstrated that the defendant was in Greece when he met with and turned over sensitive documents to the foreign agents. *Id.* at 1236-38. Thus, venue was properly established under § 3238. *Id.* at 1238-39. And in *U.S. v. Levy Auto Parts of Can.,* the Fourth Circuit held that venue was proper under § 3238 in the district of a coconspirator's arrest because the charged conspiracy "had been fully committed outside the United States, and many acts in furtherance of it had been done in Canada, Pakistan, Greece, and Iran." 787 F.2d 946, 952 (CA4 1986). Although two of the twenty-six overt acts alleged in *Levy Auto Parts* occurred in the United States, the Fourth Circuit there found that § 3238 was not rendered inapplicable because *this domestic conduct was insubstantial, tangential, and tenuously connected to the conspiracy*. *Id.* at 951-53. The obvious difference between these cases and the instant case is that *the essential criminal conduct in those cases was committed outside of the jurisdiction of any state*….

[115] *Ibid.*

Likewise, the remaining cases the government cites are also inapposite because those cases found that *§ 3238 was properly invoked when the essential criminal conduct was committed upon the high seas or outside of the jurisdiction of the United States and any conduct occurring in the United States was insubstantial*. *See U.S. v. Jensen*, 93 F.3d 667, 670 (CA9 1996) (charges resulting from operating unseaworthy vessel on high seas); *U.S. v. Erwin*, 602 F.2d 1183, 1184 (CA5 1979) (per curiam) (charges resulting from seizure of marijuana on vessel on the high seas in the Gulf of Mexico); *U.S. v. Williams*, 589 F.2d 210, 211 (CA5 1979) (charges arising from U.S. Coast Guard seizure of marijuana on vessel on the high seas with only one overt act committed in New York); *U.S. v. Bin Laden*, 91 F. Supp. 2d 600, 614 (SDNY 2000) (charges arising from bombing of U.S. embassies in Kenya and Tanzania "that occurred exclusively outside the jurisdiction of any particular state").

These cases are easily distinguishable from the present case because *the government has adduced no evidence that defendant committed the criminal conduct essential to Count 2 upon the high seas or outside of the jurisdiction of any state*…. Here, venue cannot be established in the Eastern District of Virginia based on the fact that defendant was arrested there because there is *no evidence that defendant committed the essential conduct of Count 2 outside of the jurisdiction of any State, which renders § 3231 inapplicable by its terms and its purpose*.[116]

[116] *Ibid.* 633-34 (emphasis supplied).

So too here, dictating the same conclusion.[117] Certainly the government and district court made no attempt to square a contrary result with the Venue Clause's emphatic and unequivocal command that all criminal trials except for impeachment "*shall* be held in the State where the said Crimes shall have been committed; but *when not committed within any State*, the Trial shall be at such Place or Places as the Congress may by Law have directed." Much less did the cases distinguished in *Mallory* purport to address – let alone attempt to resolve – the apparent tension.[118]

At a minimum, courts have characterized § 3738's text as "cryptic"[119] and "opaque."[120] As the Second Circuit lamented, "[a] report of the House Judiciary Committee notes that the words 'begun or' were added to the statute in 1948 'to

---

[117] The court also noted that Mallory was in the U.S. when he transmitted national defense information to Chinese agents, the "essential conduct on which venue must rest" for that offense being the information's "transmission." *Mallory*, 337 F. Supp. 3d at 632. The "essential conduct on which venue must rest" for the Count One conspiracy – as alleged, the fraudulent accessing of DFIN's and TM's computers and the unlawful obtaining of and trading on their confidential information – similarly took place in the US.

[118] As for *Miller*, it tellingly involved international parental kidnapping, an inherently multinational crime whose "crux" is "border crossing itself." 808 F.3d at 618.

[119] *Levy*, 787 F.2d at 950.

[120] *Miller*, 808 F.3d at 619.

clarify [the] scope of this section and section 3237 of this title.' Revision of Title 18, United States Code, H.R.Rep. No. 304, at A161 (1947). But unfortunately, we are able to derive little clarification as to the scope of § 3238 from the amendment."[121] And the Supreme Court has "counsel[ed]" that "close [legal] calls" on the "question" of venue

> generally ought to go to the [d]efendant, *Johnson*, 323 U.S. [at] 276 ("If an enactment of Congress equally permits the underlying spirit of the constitutional concern for trial in the vicinage to be respected rather than to be disrespected, construction should go in the direction of constitutional policy even though not commanded by it."), which some circuits have interpreted as a general mandate to construe venue narrowly.[[122]]

Given this narrow construction mandate – fortified by more "familiar principle[s]"[123] like the rule of lenity[124] and the doctrines of constitutional doubt and

---

[121] *Miller*, 808 F.3d at 619.

[122] *Eziyi*, 2023 WL 631118, at *2 (collecting cases).

[123] *Skilling*, 561 U.S. at 410-11 .

[124] Under that rule, "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity." *Yates v. U.S.*, 574 U.S. 528, 547-48 (2015).

avoidance[125] – any "tie" around § 3738's applicability to the Count One conspiracy should have "go[ne] to" Klyushin.[126] Charging the jury on high seas venue inverted those core tenets and was thus demonstrable error.[127]

In effect, a contrary holding would allow for prosecution in any of the 94 federal judicial districts where the government chooses to bring a foreign national whose conduct significantly touches, substantially impacts and place within identifiable districts in the United States.[128] That sort of breathtaking dragnet would give free rein to prosecutors' whims. It would invite the very forum shopping the

---

[125] The "constitutional doubt canon" holds that "courts should construe ambiguous statutes to avoid the need … to address serious questions about their constitutionality." *U.S. v. Davis*, 139 S. Ct. 2319, 2332 n.6 (2019).

[126] *U.S. v. Santos*, 553 U.S. 507, 514 (2008).

[127] The charging error was not harmless because the government's other venue theory – that the Count One conspiracy was properly tried in Boston as a continuing offense under 18 USC § 3237 – is also infirm, both legally and factually. At any rate, the Count One verdict was general and "may rest on [the] legally invalid [high seas venue] theory," so Klyushin's conspiracy conviction fails regardless. *U.S. v. Abdelaziz,* 64 F.4th 1, 65-66 (CA1 2023) (quoting *Skilling*, 561 U.S. at 414).

[128] *See Auernheimer*, 748 F.3d at 541 (Constitution's venue guarantees "animated" by the "danger of allowing the government to choose its forum free from any external constraints").

colonists abhorred,[129] reducing the "fundamental" and "extraordinarily important" limits the Constitution puts on venue to some pesky "technicality."[130]

That is not the law.[131] Klyushin's conspiracy conviction must be reversed.

B. The High Seas Venue Theory Prejudicially Varied the Indictment

Beyond its improper and unconstitutional application, the high seas venue theory and attending instruction foil Klyushin's Count One conviction for an additional and independent reason: its late discovery and untimely assertion prejudicially varied the indictment.[132]

---

[130] *Ibid.* 532, 540.

[131] *Cf. Smith*, 599 U.S. at 250 ("Because the crime occurred outside of New Jersey, trial in that State was proper under the Venue and Vicinage Clauses only if the crime was committed outside the limits of *any* State.") (discussing *US v. Jackalow*, 1 Black 484 (1862)).

[132] *See, e.g., U.S. v. Dellosantos*, 649 F.3d 109, 116 (CA1 2011) (explaining that a prejudicial variance occurs when "the crime charged remains unaltered, but the evidence adduced at trial proves [materially] different facts than those alleged in the indictment"; reversing conviction where indictment charged a Maine-based cocaine and marijuana conspiracy, but evidence showed only that defendants participated in a conspiracy to distribute cocaine); *U.S. v. Stein*, 429 F. Supp. 2d 633, 643 n.55 (SDNY 2006) (recognizing that a prejudicial variance could occur "if the government were to prove venue at trial on a theory different than that alleged in the indictment").

Venue was a hotly disputed issue in this case from the outset. Yet nothing leading up to the close of the government's trial presentation – from the indictment and copious motion practice around venue to the government's proposed jury instructions and eight days of testimony – even remotely implied that it intended to rely on 18 USC § 3238 to establish that prosecution was appropriate in Boston. Instead, the government – realizing that the offense conduct was only tenuously tied to Beantown – stumbled into the high seas venue theory after resting, first springing it at the literal eleventh hour: at a charge conference on the eve of summations.[133]

Starting with the indictment, it contained a total of three specific venue allegations, each incorporated by reference in all four counts. Paragraph 19 said:

> On or about October 22, 2018, ERMAKOV or another conspirator used the FA 2 Employee Credentials to obtain unauthorized access to the computer network of Filing Agent 2 *through an IP address located in Boston, Massachusetts* and to view the quarterly financial results of Capstead Mortgage Corp. ("Capstead"), the securities of which are publicly traded on the NYSE. The Capstead results had not yet been filed with the SEC or publicly disclosed. (Emphasis supplied.)

Paragraph 22 said:

> On or about October 24, 2018, ERMAKOV or another conspirator used the FA 2 Employee Credentials to obtain unauthorized access to the computer network oof Filing

[133] App:1913-22, 2089.

> Agent 2 *via another Boston IP address (collectively, "the Boston IP Addresses*"), and to view the quarterly financial results of Tesla, Inc. ("Tesla"), the securities of which are publicly traded on the NASDAQ. (Emphasis supplied.)

Paragraph 45 said, in part:

> On or about October 24, 2018, in the District of Massachusetts and elsewhere, the defendants … [fraudulently transmitted] the FA 2 Employee Credentials … *via the Boston IP Addresses*[] to one or more computer servers outside of Massachusetts in order to obtain unauthorized access to the computer network of Filing Agent 2. (Emphasis supplied.)

These allegations, legally required or not,[134] plainly intended and served to assert conduct-based venue in Boston. Nowhere did the indictment provide the slightest inkling that the government also intended to assert high seas venue under § 3238.[135]

---

[134] *Cf., e.g., U.S. v. Rudolph*, No. 22-cr-012-WJM, 2022 WL 1225314, at *5-*6 (D. Colo. Apr. 26, 2022)

[135] *Cf., e.g., U.S. v. Hassanshahi*, 185 F. Supp. 3d 55, 56-57 (D.D.C. 2016) (indictment "assert[ed] two separate bases for venue," stating that "venue is proper under § 3237(a) because 'the conduct alleged … occurred within the District of Columbia and elsewhere,' and also that venue is proper under § 3238, because 'the conduct alleged … began outside the jurisdiction of any particular state or district of the United States, but within the jurisdiction of the United States'").

Klyushin relied on the indictment's conduct-based venue allegations and designed his defense accordingly, to discredit them. Prior to trial, he thus moved to exclude government-proffered geolocation evidence purporting to trace passthrough IP addresses to Boston, arguing that it was unauthenticated and unreliable hearsay lacking suitable expert foundation and violating the Confrontation Clause. The government vigorously opposed, but ultimately relented and decided not to offer the contested geolocation evidence, saying it would link to Boston by other means – physically link to Boston – computer servers associated with the passthrough IP addresses.[136]

The heated litigation around the geolocation issue – one even the government termed "gnarly"[137] – left no doubt as to conduct-based venue's primacy at the upcoming trial. And again, the accompanying motion practice – like the indictment before it – did not even begin to hint at any alternate venue theory.[138] Nor did the

---

[136] *See*, *e.g.*, App:173-74; App:216-18; Doc.132; Doc.136; App:591-95; App:298-305.

[137] App:299.

[138] *Cf. Miller*, 806 F.3d at 611-12 (in opposing pretrial motion, government represented that trial evidence would establish venue "under either of two … statutes: § 3237 or § 3238 of title 18," informing court after ruling that it would proceed "under § 3238 only").

proposed venue instruction – relying exclusively on § 3237 – the government submitted before trial.[139] As the court would later remark:

> It was never, never, never in doubt that once we had the debate about the Maxmind [geolocation] application, which was several weeks before trial, it was clear that there was going to be a debate about venue. So it was not something that they [the defense] brought up at the last minute in openings. It was fully freighted. …[140]

Continuing to rely on the indictment's allegations and the government's representations in opposing the venue-oriented geolocation motion, Klyushin "opened" by assailing his prosecution in Boston, arguing the conduct ascribed to him had no meaningful connection to Beantown and the case didn't belong there.[141] Meanwhile, the government presented voluminous documentary evidence, and testimony from a DFIN-retained forensic analyst, suggesting that packets of information had passed between the conspirators in Russia and stateside filing agent computers through servers associated with Boston-based IP addresses.[142] The

[139] App:367-68.

[140] App:1921.

[141] *See, e.g.*, App:1918-19.

[142] *See, e.g.*, App:2504-05.

government even went so far as to call, over strenuous objection, a surprise witness from North Carolina – a former employee of a company associated with the IP addresses – to shore up that contention.[143]

For Klyushin's part, he built his defense around countering this body of proof. As the government itself would later concede: "The trial defense in this case was clearly that there was no server, there was no connection at all to Boston, there was no wire here, no nothing."[144]

Yet after all that – after all the time and energy each party had devoted to developing the presence or absence of essential Boston offense conduct sufficient to satisfy § 3237 – the government pulled the rug out from under the defense at what was literally the last moment. Following a half hour of lunchtime research between the close of its case and the charge conference,[145] the government sandbagged Klyushin and blindsided the court by "popping"[146] the entirely new and novel

---

[143] *See, e.g.*, App:2504-07.

[144] App:2546.

[145] App: 1914, 1918, 2102.

[146] App:1914 ("THE COURT: All right, you're just popping it on me."); App:1915 ("THE COURT: … This is a surprise pop …"); App:1916 ("THE COURT: I tell you what: You're popping it on me. You're popping it on the

supposition that venue was proper under § 3738, the "not often used"[147] high seas statute, which required *no* Boston conduct whatever.

In reluctantly[148] accommodating this (errant) afterthought[149] – and partially instructing the jury in kind – the court effectively charged Klyushin's defense out of the case as to Count One, all but directing a conspiracy verdict for the government. It thereby condoned a prosecutorial bait-and-switch – intentional or not[150] – that severely and "unfair[ly]"[151] misled the defense.

Had counsel known the government would claim that a Boston trial was proper simply because Klyushin was first brought there from overseas, they never would have defended on venue grounds – much less made venue what the

---

defense.").

[147] App:1917 (prosecutor so conceding).

[148] *See* App:1963 ("THE COURT: Can I also say, there's a really solid argument you [the government] waived [§ 3238] by not submitting a jury instruction on it.").

[149] In a considerable understatement, the government acknowledged that its 180-degree reversal was "late" and "apologize[d that] we didn't raise it [§ 3738] earlier." App:1913.

[150] *Cf.* App:1919 ("MR. KOSTO: We would not have put in as much venue as we did if this [§ 3238] were in our heads, and it wasn't, your Honor.").

[151] *Cf.* App:1920.

government's own lawyers couched as the defense's thrust. They would have chosen some other defense theory or, in the absence of one, aggressively pursued a plea deal and strongly advised their client to take it.

If that is not a textbook example of a prejudicial variance, then nothing is.[152] Klyushin's conspiracy conviction falters on this additional ground.[153]

C. Conclusion

Having charged and tried the case exclusively on a continuing offense theory under 18 USC § 3237, the government unfairly ambushed Klyushin with an alternate high seas venue theory under § 3238. But that theory prejudicially varied the indictment and was palpably inapplicable – legally, logically, constitutionally –

---

[152] *See U.S. v. Glenn*, 828 F.2d 855, 859-60 (CA1 1987) (Breyer, J.) (noting that prejudice results when a variance allows the government to try a defendant in an improper forum or one in which his conspiracy did not take place; reversing conviction where evidence showed separate marijuana and hashish conspiracies rather than single, integrated drug conspiracy indictment alleged).

[153] *Cf. U.S. v. Nguyen*, 507 F. App'x 64, 66-67 (CA2 2013) (unpublished) ("venue arguments" first "articulated" in government's "closing and rebuttal" were supported by evidence and consistent with "core of criminality" alleged, even though their underlying "facts" were "not set out" in indictment; defendant "should have anticipated the use of these [venue] proofs," so any variance "could not have misled" or prejudiced him).

where essential conspiratorial conduct took place in identifiable American states and districts. Klyushin's Count One conviction crumbles in consequence.

V. THE DISTRICT COURT REVERSIBLY ERRED IN ITS COUNT FOUR (SUBSTANTIVE STOCK FRAUD) VENUE INSTRUCTION

Over ongoing objection[154] that the securities fraud statute has its own specific venue provision,[155] the district court erroneously[156] instructed the jury – at the government's request – to evaluate Count Four for venue purposes under 18 USC § 3237, the general default statute for continuing offenses.[157] The error was prejudicial because the evidence was legally insufficient for a properly instructed jury to find stock fraud venue established in Boston. At most, Boston served as a passthrough for the confidential information misappropriated from the filing agents that eventually led to fraudulent stock trades. Absent evidence that those trades themselves were executed in Boston, such anterior conduct fails to confer

---

[154] App:1936-42; App:1944-46; App:2094-95; App:2521-22.

[155] *See* 15 USC § 78aa.

[156] *See*, *e.g.*, *Mallory*, 337 F. Supp. 3d at 633 (calling it "well-settled that when a criminal offense does *not* include a specific venue provision, venue must be determined from the nature of the crime alleged and the acts constituting it") (emphasis supplied); *Royer*, 549 F.3d at 895 (CA2 2008); *Geibel*, 369 F.3d at 96.

[157] App:1360.

substantive stock fraud venue in Massachusetts as a matter of law.[158] Since "venue must be laid in a district where all the counts" in a single, multi-count indictment "may be tried,"[159] this Court must reverse Klyushin's conviction in its entirety.

VI. THE DISTRICT COURT ERRED IN INSTRUCTING THE JURY TO FIND VENUE ONLY BY PREPONDERANT EVIDENCE, RATHER THAN BEYOND A REASONABLE DOUBT

Though the argument is currently foreclosed,[160] Klyushin continues to claim[161] for potential higher review that venue – as a "finding of fact" on which an "increase in a defendant's authorized punishment" is "contingent"[162] – must be pleaded in the indictment and proved beyond a reasonable doubt under the

[158] *See Geibel*, 369 F.3d at 696-97; *Cabrales*, 524 U.S. at 3-4, 6-7, 10.

[159] *Royer*, 549 F.3d at 893-94; *see also Saavedra*, 223 F.3d at 89.

[160] *See, e.g.*, *U.S. v. Salinas*, 373 F.3d 161, 163-64 (CA1 2004).

[161] App:1698; App:2261-62; App:2569.

[162] *U.S. v. Booker*, 543 U.S. 220, 231 (2005).

Constitution's Fifth and Sixth amendments.[163] Proof beyond a reasonable doubt also accords with early American historical practice around the venue requirement.[164]

VII. THE INDICTMENT FAILED TO CHARGE A COGNIZABLE STOCK FRAUD CRIME – AND THE DISTRICT COURT ERRED IN INSTRUCTING THE JURY OTHERWISE – BECAUSE IT DID NOT AND COULD NOT ALLEGE THAT KLYUSHIN, A CORPORATE OUTSIDER, OWED OR BREACHED A FIDUCIARY OR SIMILAR DUTY OF DISCLOSURE TO EITHER MARKET PARTICIPANTS OR ANY SOURCE OF INFORMATION ASSERTEDLY STOLEN BY HACKING

Having plausibly accused Klyushin of computer and wire fraud, the government piled on by dressing up the same underlying hack-and-trade scheme in a "novel"[165] theory of stock fraud: namely, that a band of corporate outsiders engaged in "deception" simpliciter – criminally violating federal securities law – by hacking into filing agent computers, illicitly harvesting employee login credentials and using them to steal confidential business information for trading advantage.

---

[163] App:2254.

[164] *See, e.g.*, *Lawless v. State*, 72 Tenn. 173, 180, 182 (1879); *U.S. v. Wilson*, 28 F. Cas. 699, 710 (C.C.E.D. Pa. 1830).

[165] *SEC v. Dorozhko*, 606 F. Supp. 2d 321, 324 (SDNY 2008) (*Dorozhko I*), *vacated*, 574 F.3d 42 (CA2 2009) (*Dorozhko II*).

Never recognized by the Supreme Court or this one in almost 90 years of securities law experience, that belt-and-suspenders approach belies the "essential component" and "entire construct" at the "heart" of "insider trading regulation": a "breach of a fiduciary" or similar "duty to disclose or abstain that coincides with a [stock] transaction."[166]

If sustained, the government's envelope-pushing position – and the corresponding jury instruction the district court gave over continued objection[167] – would radically expand the scope of § 10(b) liability, elevating every larceny by false pretenses that somehow touches securities into criminal insider trading. To avoid that intolerable result, this Court should rebuke the government's test case and

[166] *Ibid.* 338-41.

[167] App:2243-52.

dismiss Count Four (plus Count One's concomitant securities fraud object)[168] for failure to allege a viable stock fraud offense.[169]

A. Legal Background

As relevant here, § 10(b) of the 1934 Securities Exchange Act "proscribes (1) using any deceptive device (2) in connection with the purchase or sale of securities, in contravention of rules prescribed by the [Securities and Exchange] Commission."[170] Rule 10b-5, prescribed by the SEC in turn, outlaws, among other

[168] Since the jury's general verdict on Count One's multi-object conspiracy "may rest on a legally invalid theory" – one contemplating a duty-less securities fraud predicate – Klyushin's conspiracy conviction founders in its entirety. *Abdelaziz*, 64 F.4th at 65-66 (quoting *Skilling.*, 561 U.S. at 414). Regardless, the whole point of the Count One conspiracy as alleged – its underlying motive and ultimate goal; the "trade" part of the overall hack-and-trade scheme holding the case together – was trading on information stolen from the filing agents. App:2246-47 (court charging jury that core conduct "involved" Klyushin or a co-schemer "misrepresenting" their "identity online to access computer systems to obtain material nonpublic information to trade on the confidential information"). So the errors tainting Count Four – theoretical and instructional – infect Count One with spillover prejudice, scuttling it in full. *E.g.*, *U.S. v. Martinez*, 994 F.3d 1, 14-15 (CA1 2021).

[169] In rebuffing this argument before trial, Judge Saris effectively punted the issue to this Court. To that end, she called her decision a "placeholder to see [how] the First Circuit" rules and ventured that it could "potentially … go a different way." App:109-110.

[170] *U.S. v. O'Hagan*, 521 U.S. 642, 651 (1997).

things, "mak[ing] untrue statements of material facts" or "omit[ting] to state material facts" in connection with "the purchase and sale of securities."[171]

While intended to "insure honest securities markets and thereby promote investor confidence,"[172] these provisions are not "a broad federal remedy for all fraud"[173] or a "blanket prohibition on illicit schemes that somehow involve securities transactions."[174] They do "*not* reach all structural disparities in information that result in securities transactions"[175] and "must not be construed so broadly as to convert every common-law fraud that happens to involve securities into a [§ 10(b)] violation."[176] In particular, the Supreme Court has long emphasized that a general "duty to disclose under § 10(b) does not arise from the mere possession of nonpublic market information,"[177] however acquired.

---

[171] App:50.

[172] *O'Hagan*, 521 U.S. at 658.

[173] *Marine Bank v. Weaver*, 455 U.S. 551, 556 (1982).

[174] *Dorozhko I*, 606 F. Supp. 2d at 335.

[175] *Ibid.* (emphasis supplied).

[176] *SEC v. Zandford*, 535 U.S. 813, 820 (2002).

[177] *Chiarella*, 445 U.S. at 229, 235.

Over 90 years of interpretation since the Act's passage, the Court has "established that there are two complementary theories of insider trading liability"[178] under § 10(b) and accompanying Rule 10b-5. Under the "**traditional**" or "**classical**" theory, a "corporate insider" – permanent or temporary – "trades in the securities" of their corporation on the basis of "material, nonpublic information."[179] Such trading counts as "deceptive" under § 10(b) because a "relationship of trust and confidence exists" between a corporation's shareholders and insiders who obtain "confidential information by reason of their [corporate] position."[180] And that relationship gives rise to a "duty to disclose" or "abstain from trading" so as to prevent corporate insiders from taking unfair advantage of uninformed stockholders – the counterparties to a purchase or sale.[181]

---

[178] Donna M. Nagy, *Insider Trading and the Gradual Demise of Fiduciary Principles*, 94 Iowa L. Rev. 1315, 1316 (May 2009) (Nagy).

[179] *O'Hagan*, 521 U.S. at 651-52.

[180] *Ibid.* 652.

[181] *Ibid.*; *see Chiarella*, 445 U.S. at 228 ("one who fails to disclose material information prior to the consummation of a transaction commits fraud only when … under a duty to" disclose).

Under the "**misappropriation**" theory, on the other hand, a malefactor "misappropriates confidential information for securities trading purposes, in breach of a duty owed to the [information's] source."[182] On that theory, the Court elaborated, a fiduciary's

> undisclosed, self-serving use of a principal's information to purchase or sell securities, in breach of a duty of loyalty and confidentiality, defrauds the principal of the exclusive use of that information. In lieu of premising liability on a fiduciary relationship between company insider and purchaser or seller of the company's stock, the misappropriation theory premises liability on a fiduciary-turned-trader's deception of those who entrusted him with access to confidential information.[183]

At the "heart"[184] or "core"[185] of both established theories – insider trading's "essential component"[186] and "entire construct"[187] – is the "requirement"[188] of a

---

[182] *O'Hagan*, 521 U.S. at 652.

[183] *Ibid.*

[184] *Dorozhko I*, 606 F. Supp. 2d at 340.

[185] Nagy, 94 Iowa L. Rev. at 1316.

[186] *Dorozhko I*, 606 F. Supp. 2d at 338.

[187] *Ibid.* 340-41.

[188] *Ibid.* 341; Elizabeth A. Odian, SEC v. Dorozhko*'s Affirmative*

"fiduciary"[189] relationship or similar duty of trust and confidence.[190] As the Supreme Court squarely put it: "The classical theory targets a corporate insider's breach of duty to shareholders with whom the insider transacts; the misappropriation theory [forbids] trading on the basis of nonpublic information by a corporate 'outsider' in breach of a duty owed not to a trading party, but to the [information's] source."[191]

In sum, breach of a fiduciary or similar duty serves as the uniform "basis" or "predicate[]" for stock fraud liability under Supreme Court and First Circuit precedent; absent a fiduciary or similar breach, there is no deception within § 10(b)'s meaning and thus no insider trading violation.[192] Stated simply, the high court has

---

Misrepresentation Theory of Insider Trading: An Improper Means to a Proper End, 94 Marq. L. Rev. 1313, 1313 (Summer 2011) (Odian).

[189] *Dorozhko I*, 606 F. Supp. 2d at 338, 340-41.

[190] *See, e.g.*, *SEC v. Rocklage*, 470 F.3d 1, 6 (CA1 2006) ("when the trading individual owes no fiduciary duty to the stockholders…. there can be no insider trading liability under the classical theory"); *U.S. v. Kanodia*, 943 F.3d 499, 506 (CA1 2019) ("Because the government prosecuted Kanodia on a misappropriation theory of insider trading, the jury needed to find that Kanodia breached a duty of trust and confidence owed to a corporate insider").

[191] *O'Hagan*, 521 U.S. at 652-53.

[192] *Dorozhko I*, 606 F. Supp. 2d at 323-24, 330, 337-39.

"explicit[ly] dictate[d] that fiduciary principles underlie the offense of insider trading"[193] – of *any* stripe.[194]

B. The Novel and Invalid Stock Fraud Theory Here

In the case at hand, defendants are "true" corporate outsiders – not claimed to have "owed" or breached any fiduciary-type duty to either "market participants" or confidential information "source[s]"[195] – who allegedly hacked into filing agent computers, extracted employee login credentials and used them to steal material nonpublic information for trading advantage. Open and shut case, right?[196] Under controlling law, defendants may face prosecution for wire and computer fraud,[197] but not insider trading. No duty or breach, no securities fraud.

---

[193] Nagy, 94 Iowa L. Rev. at 1319.

[194] *Ibid.* 1323-24 & n.35 (calling fiduciary-like relationship "essential" to "either" recognized Supreme Court stock fraud theory (classical and misappropriation)).

[195] *Dorozhko I*, 606 F. Supp. 2d at 336.

[196] *See* Odian, 94 Marq. L. Rev. at 1344 (confirming that "computer hacking does not fit within the contours of classical insider trading or the fraud on the source theory adopted by the Supreme Court in *O'Hagan*").

[197] *Dorozhko I*, 606 F. Supp. 2d at 323 & n.2 (recognizing that the "conduct alleged might violate the computer fraud statute, 18 USC § 1030(a)(4), and the mail and wire fraud statutes, 18 USC § 1341 *et seq.*"); *see also id.* 324 (finding "sufficient

Well, not so fast. Not content with what binding precedent explicitly authorizes, the government resorted to unwarranted overkill by conjuring a whole "new" species of "insider,"[198] previously unknown in decades of Supreme Court and First Circuit securities practice. More precisely, the government appeared to contend that defendants engaged in "deception" as commonly understood by remotely impersonating filing agent employees – the same conduct charged in counts One through Three – in connection with securities purchases and sales, also rendering them criminally liable for stock fraud. In essence, the government thus seemed to suggest, any deceit involving stock – "any fraudulent scheme that contains the requisite nexus to a securities transaction"[199] – automatically violates § 10(b).

---

basis to conclude that Dorozhko's hack violated the Computer Fraud and Abuse Act" and "wire fraud statute"); Robert A. Prentice, *The Internet and Its Challenges for the Future of Insider Trading Regulation*, 12 Harv. J.L. & Tech. 263, 297-98 (1999) (failing "nontraditional" arguments, insider trading based on hacked information "would have to be punished … via mail fraud, wire fraud, simple theft, or other comparable statutes").

[198] Odian, 94 Marq. L. Rev. at 1313.

[199] *Dorozhko I*, 606 F. Supp. 2d at 336.

Courts and commentators have condemned this novel "hack-and-trade" theory as "greatly extend[ing] the reach of the SEC's policing power"[200] and lacking "doctrinal foundation."[201] After all, § 10(b) "deception" is a term of art glossed by the Supreme Court over some 90 years,[202] and it *consists of* – actually *resides in* – the existence and breach of a fiduciary-type duty.[203] Accordingly, because Klyushin owed no such duty to any information source – either the filing agents or their corporate clients – or "to those he transacted with in the market," he could not have breached one "in connection with the purchase or sale of a security."[204] It follows

---

[200] Odian, 94 Marq. L. Rev. at 1313.

[201] Nagy, 94 Iowa L. Rev. at 1316.

[202] *Dorozhko I*, 606 F. Supp. 2d at 330 n.8; *see Stoneridge Inv. Partners, LLC v. Scientific Atl., Inc.*, 552 U.S. 148, 162 (2008) ("Section 10(b) does not incorporate common-law fraud into federal law.").

[203] *Dorozhko I*, 606 F. Supp. 2d at, *e.g.*, 330 (Supreme Court cases interpreting § 10(b) have "established that a device, such as a scheme, is not 'deceptive' unless it involves breach of some duty of candid disclosure"); *accord*, *e.g.*, *id.* 330 n.8 (§ 10(b) deception "necessarily involve[s] the breach of a fiduciary or similar duty"); *id.* 330 (breaching a "fiduciary duty of disclosure is a required element of any 'deceptive' device under § 10(b)"); *see generally id.* 338-39; Nagy, 94 Iowa L. Rev. at 1360-61 (*O'Hagan* made clear that it is "the insider trader's breach of trust and loyalty" that "constitutes the fraud under Rule 10b-5").

[204] *Dorozhko I*, 606 F. Supp. 2d at 324.

that his alleged "'hacking and trading' does not amount to a violation of § 10(b) and Rule 10b-5."[205]

As one judge, quoting a scholarly article,[206] explained at some length:

> A … hacker who breaches the computer security walls of a large publicly held corporation and extracts nonpublic information may … trade and tip without running afoul of the insider trading rules. The … hacker may be liable for the conversion of nonpublic information under other laws, but the insider trading laws themselves appear not to prohibit the … hacker from trading or tipping on the basis of the stolen information. This is because there was no breach of a duty of loyalty to traders under the classic theory or to the source of the information under the misappropriation theory.[207]

By eliminating the crux of both § 10(b) deception and insider trading itself – the "requirement" of a fiduciary-type breach – the government's unorthodox "hack-and-trade" theory thus conflated theft and stock fraud, "undo[ing] decades of Supreme Court" and First Circuit "precedent" and "rewrit[ing] the law as it has

---

[205] *Ibid.*

[206] *See* Kathleen Coles, *The Dilemma of the Remote Tippee*, 41 Gonz. L. Rev. 181, 221 (2005-06).

[207] *Dorozhko I*, 606 F. Supp. 2d at 341-42.

developed."[208] Even given "parallel coinciding criminal conduct" that may "amount[] to wire" and computer fraud, "there can be no 'deception,' and therefore no liability under § 10(b), absent the existence and breach of a fiduciary" or comparable duty.[209] Contrary to the government's apparent supposition, "§ 10(b) does not reach all structural disparities in information that result in securities transactions, only those disparities obtained by dint" of a "fiduciary" or equivalent "breach."[210]

To our knowledge, only one stray court swims against the prevailing academic and judicial tide. In *Dorozkho II*,[211] a civil enforcement action, a panel of the Second Circuit Court of Appeals made the surprising and "unprecedented"[212] assertion that Supreme Court securities precedent, closely read, strictly requires a fiduciary-type relationship only in cases involving omission or nondisclosure – and, concomitantly, that it does not foreclose § 10(b) liability without one in cases of affirmative

---

[208] *Ibid.* 323, 340-41, 343.

[209] *Ibid.* 338.

[210] *Ibid.* 335.

[211] 574 F.3d 42.

[212] Odian, 94 Marq. L. Rev. at 1313.

misrepresentation. (Remotely impersonating a filing agent employee would presumably or ostensibly fit the latter bill in the Second Circuit's view.) Twelve years later, in July 2021, a different panel of the same court summarily extended *Dorozkho II* to the criminal context in a single unreasoned sentence.[213] The Second Circuit's "approach"[214] is severely "flawed"[215] and should not prevail in this one – especially on the facts and circumstances presented here.

C. The Second Circuit's Peculiar Take on Securities Fraud is Unprecedented, Unsound and Unconstitutional as Applied in this Case

This Court should reject the new species of stock fraud liability the Second Circuit invented in *Dorozkho II* and expanded in *Khalupsky*, holding it unfounded, illegitimate, and unconstitutional as applied to Klyushin – and dismissing counts Four and One in consequence.

---

[213] *U.S. v. Khalupsky*, 5 F. 4th 279, 290 & n.30 (CA2).

[214] Odian, 94 Marq. L. Rev. at 1313.

[215] *Ibid.*; *see Dorozkho II*, 574 F.3d at 45 (conceding that imposing § 10(b) liability "against defendant – a corporate outsider who owed no fiduciary duties to the source of the information – is not based on either of the two generally accepted theories of insider trading").

First, the *Dorozkho II* panel's analysis rests on a demonstrably faulty premise: that statutory interpretation begins by consulting applicable caselaw.[216] In fact, as *Dorozkho I* properly recognized,[217] the cardinal tenet of statutory interpretation is that construction both starts and ends – absent grievous ambiguity – with the text of the operative statute itself.[218]

Second, the text of Rule 10b-5(b) juxtaposes and equates affirmative misrepresentations and material omissions or nondisclosures,[219] treating them as coterminous and qualitatively synonymous for purposes of securities fraud liability. Thus, far from supplying a textual basis to distinguish the two, the rule's plain

---

[216] 574 F.3d at 46 ("[i]n construing the text of any federal statute, we first consider the precedents that bind us as an intermediate appellate court").

[217] 606 F. Supp. 2d at 327 ("As in all cases involving statutory interpretation, the appropriate starting point is the text of the statute itself.") (citing *Cent. Bank of Denver v. First Interstate Bank of Denver*, 511 U.S. 164, 172-73 (1994), *superseded by statute on other grounds as stated in SEC v. Fehn*, 97 F.3d 1276, 1280 (CA9 1996)).

[218] *Ibid.* ("In addressing the elements of a cause of action under Section 10(b) and Rule 10b-5, we turn first to the language of § 10(b), for the starting point in every case involving construction of a statute is the language itself") (quoting *Ernst & Ernst v. Hochfelder*, 425 U.S. 185, 197 (1976)) (cleaned up).

[219] By its terms, Rule 10b-5(b) makes it "unlawful for any person, directly or indirectly," to "make any untrue statement of a material fact or to omit to state a material fact" in "connection with the purchase or sale of any security."

language contradicts if not precludes any effort to do so. If omission liability requires a fiduciary-type breach, as even the *Dorozkho II* panel acknowledged, it follows that liability for affirmative misrepresentations does as well.

Third, language aside, settled law further belies the artificial distinction the *Dorozkho II* panel tried to draw. In *Santa Fe Indus. v. Green*, a 45-year-old case the panel conspicuously ignored, the Supreme Court pointedly "defined 'deception' as proscribed in § 10(b) as the making of a material misrepresentation *or* the non-disclosure of material information *in violation of a duty to disclose*."[220]

Fourth, beyond confounding law and language, any § 10(b) distinction between misrepresentations and omissions also defies simple common sense. Take the conduct charged here. Remotely impersonating a filing agent employee – virtually passing yourself off as that individual – may be one man's affirmative misrepresentation but another's material omission – *i.e.*, failing to disclose the digital masquerade. They're two sides of the same functional coin. Similarly, while contending the former constitutes an affirmative misrepresentation and thus an actionable deception, the Second Circuit concedes uncertainty whether alternate,

[220] *Dorozkho I*, 606 F. Supp. 2d at 330 (citing 430 U.S. 462, 470 (1977)) (emphasis supplied).

equally blameworthy forms of hacking – for example, using malware or SQL injection[221] to exploit a weakness in electronic code and gain unauthorized access – would qualify under its idiosyncratic rationale.[222] A coherent and administrable statutory scheme does not pin liability on arbitrary labels, semantic abstractions or the technical means a hacker happens to choose to infiltrate a protected computer. Especially when liability carries the risk of years in prison.

Fifth, speaking of years in prison, the *Dorozkho II* panel hastened to qualify the duty-free, deception-as-insider-trading theory it improvised, pregnantly confining its unique approach to the "facts presented" and deeming them "sufficient to maintain a civil enforcement action."[223] Even if *Dorozkho II* were defensible as a *sui generis* outlier (and it isn't), it by no means follows that the *Khalupsky* panel appropriately imported its solitary spin wholesale into the criminal context 12 years later – much less summarily, without explanation, examination or analysis, in a

[221] According to the *Khalupsky* panel, SQL injection is a technique that enables intruders to "glean the architecture of [a] hacked computer system, identify vulnerabilities, and extract data." 5 F.4th at 291.

[222] *See Dorozhko II*, 574 F.3d at 50-51; *Khalupsky*, 5 F.4th at 291.

[223] 574 F.3d at 49-50 n.6.

single unsupported sentence.[224] After all, while § 10(b) may be construed "flexibly to effectuate its remedial purposes"[225] in the civil setting, it is fundamental that penal laws are "construed strictly."[226] And when a statute has both criminal and civil application, the Supreme Court recently reiterated, it must be interpreted uniformly.[227]

Sixth, all of this is true even if *Dorozkho II* and *Khalupsky* come from what the government extolled below as the nation's "preeminent court for securities law."[228] Indeed, the Supreme Court *reversed* the Second Circuit in the seminal case in this area,[229] *rejecting* the idea that federal securities law broadly prohibits exploitation of "any structural advantage in information that was wrongly obtained"

---

[224] *See* 5 F.4th at 290 & n.30.

[225] *Dorozhko II*, 574 F.3d at 47.

[226] *E.g.*, *U.S. v. Smith*, 500 F.3d 27, 32 n.5 (CA1 2007); *cf.* Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* 364-66 (2012) (denouncing, as an "open invitation to engage in 'purposive' rather than textual interpretation," the "false notion that remedial statutes should be liberally construed").

[227] *Sessions v. Dimaya*, 138 S. Ct. 1204, 1217 (2018).

[228] App:88.

[229] *See Chiarella*, 445 U.S. 222.

– even in the absence of a fiduciary-like breach.[230] As at least one jurist and several academics have observed, hack-and-trade "essentially seek[s] to revive" or "resurrect" that discredited view, effectively "extend[ing] § 10(b) liability to any situation" where information is stolen or otherwise illicitly acquired.[231] Nor was *Chiarella* the last time the Supreme Court had to rein in the Second Circuit's expansive interpretation of federal penal statutes[232] – including those related to securities fraud.[233]

Seventh, it bears emphasis that the undefined, "amorphous term 'deceptive device,'" as used in § 10(b), is at least "ambiguous."[234] And the SEC, in the many years before or since *Dorozkho II*, has never exercised its congressionally delegated authority to promulgate a rule declaring hacking-and-trading simpliciter – without a

---

[230] *Dorozkho I*, 606 F. Supp. 2d at 333-34.

[231] *Ibid.* at 333-34, 336 & n.10. ,

[232] *See, e.g.*, *Ciminelli v. U.S.*, 598 U.S. 306 (2023); *Percoco v. U.S.*, 598 U.S. 319 (2023) *Marinello v. U.S.*, 138 S. Ct. 1101 (2018); *Sekhar v. U.S.*, 570 U.S. 729 (2013).

[233] *See Salman v. U.S.*, 580 U.S. 39 (2016), *abrogating U.S. v. Newman*, 773 F.3d 438 (CA2 2014).

[234] *U.S. v. McGee*, 763 F.3d 304, 313-15 (CA3 2014) (citing *Chiarella*, 445 U.S. at 226); *cf. Zandford*, 535 U.S. at 819-20 (dubbing § 10(b) "ambiguous").

corresponding duty breach – prohibited securities activity.[235] This hiatus starkly contrasts with Rule 14e-3(a), a 1980 provision targeting tender offer fraud that shows the SEC clearly knows how to jettison any fiduciary requirement – in language the world will understand – when it wants to.[236] The "tie" therefore should have "go[ne] to the defendant" in the criminal context,[237] the rule of lenity – the "familiar principle"[238] that "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity"[239] – counseling rejection, not extension, of *Dorozkho II*'s duty-less hack-and-trade concoction in *Khalupsky*.

---

[235] *Cf.*, *e.g.*, 17 CFR § 240.10b5-2(b) (clarifying the circumstances giving rise to a "duty of trust or confidence" following *O'Hagan*'s recognition of misappropriation liability); 15 U.S.C. § 78t(e) (amending Act to abrogate *Cent. Bank* and restore SEC's ability to sue individuals for knowingly aiding and abetting securities fraud).

[236] As *O'Hagan* explained, Rule 14e-3(a) "creates a duty to disclose material non-public information, or abstain from trading in stocks implicated by an impending tender offer, *regardless of whether such information was obtained through a breach of fiduciary duty*." 521 U.S. at 667-70.

[237] *Santos*, 553 U.S. at 514.

[238] *Skilling*, 561 U.S. at 410-11.

[239] *Yates.*, 574 U.S. at 547-48.

Eighth, this conclusion rings doubly true in the circumstances at hand. Note here that *Khalupsky* was not decided until July 2021, well after the end of the conduct charged in counts One and Four, Klyushin's arrest and his indictment's return. To that point, "no federal court" in almost 90 years' experience with the Act had "*ever* held that those who steal material nonpublic information and then trade on it" *criminally* "violate § 10(b)."[240] As such, and especially without an SEC rule addressing the issue, Klyushin had no reason to suspect – and certainly could not have known – that hacking a computer to extract valuable trading information, whether by impersonating an employee or any other means, could trigger penal liability and years of prison for securities fraud *in the absence of a fiduciary relationship or similar duty of trust and confidence*.

Because § 10(b) has already been found ambiguous[241] – and otherwise fails to "define the criminal offense with sufficient" precision for "ordinary people" to "understand" – Klyushin thus lacked prior inkling or notice that the pre-*Khalupsky* behavior ascribed to him amounted to criminally "prohibited" insider trading.[242] As

---

[240] *Dorozkho I*, 606 F. Supp. 2d at 339.

[241] *E.g.*, *McGee*, 763 F.3d at 313-15.

[242] *Kolender v. Lawson*, 461 U.S. 352, 357 (1983).

interpreted after-the-fact by the panel in *Khalupsky* and the government here, the Act therefore raises serious "vagueness concerns"[243] and "encourage[s] arbitrary and discriminatory enforcement,"[244] offending due process, violating the Fifth Amendment and arguably rendering it unconstitutional as applied to Klyushin.

To alleviate these substantial concerns, basic principles of statutory construction – not just the rule of lenity, but also the canons favoring avoidance of both difficult constitutional questions and constitutionally doubtful constructions[245] – call for dismissing counts Four and One. This is especially so because larceny by false pretenses, the gist of the conduct the government dressed up as securities fraud, is a traditional state law crime. And Congress does not significantly disrupt the delicate balance between "federal and state criminal jurisdiction" without a "clear statement" of intent to do so.[246] Nothing in § 10(b) or Rule 10b-5(b) offers any such indication.

---

[243] *U.S. v. Scott*, 979 F.3d 986, 993 (CA2 2020).

[244] *Lawson*, 461 U.S. at 993.

[245] *See, e.g.*, *U.S. v. Davis*, 139 S. Ct. 2319, 2332-33 & n.6 (2019).

[246] *Bond v. U.S.*, 572 U.S. 844, 858-59 (2014); *cf. Santa Fe Indus.*, 430 U.S. at 478-80.

D. Conclusion

A remedy without an incremental wrong and a solution in search of a problem, the unconventional hack-and-trade theory of stock fraud floated in this case fills a phantom enforcement gap amply covered by the wire and computer fraud statutes.[247] Improperly substituting dictionary definitions for a well understood term of art – § 10(b) "deception"[248] – and eradicating stock fraud's linchpin – breach of a fiduciary or similar duty of trust and confidence – the government's maximalist position upends decades of settled precedent and drastically expands federal prosecutorial power. A study in "overdeterrence"[249] and a recipe for "overcriminalization,"[250] it makes inside traders out of every common thief whose ultimate goal is securities profit.

---

[247] Indeed, 18 U.S.C. §§ 1348-49, statutes carrying 25-year maximum penalties, also appear to prohibit the conduct at issue. *See* Nagy, 94 Iowa L. Rev. at 1322 n.29.

[248] Compare *Dorozkho I*, 606 F. Supp. 2d at 330 n.8 with *Dorozkho II*, 574 F.3d at 50, 51.

[249] *Ruan v. U.S.*, 597 U.S. 450, 459 (2022) (Breyer, J.).

[250] *Yates*, 574 U.S. at 569 (Kagan, Scalia, Kennedy and Thomas, JJ., dissenting).

Because this extreme approach lacks any basis in – indeed flatly contradicts – controlling law, the Court should dismiss counts Four and One for failure to charge cognizable § 10(b) violations. Any other outcome, as one commentator aptly noted, is an invitation to "revisionism and results-oriented decisionmaking."[251]

CONCLUSION

For the foregoing reasons, Klyushin's convictions should be vacated.

Respectfully submitted,
Vladislav Klyushin
By his Attorneys,

/s/ Maksim Nemtsev
Maksim Nemtsev
20 Park Plaza, Suite 1000
Boston, MA 02116
(617) 227-3700 (Telephone)
max@mnpc.law

/s/ Marc Fernich
Marc Fernich
800 Third Avenue, Floor 20
New York, NY 10022
(212) 446-2346 (Telephone)
maf@fernichlaw.com

[251] Nagy, 94 Iowa L. Rev. at 1320-21.

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMIT

1. This document does not currently comply with Fed. R. App. P. 32(a)(7)(B) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f), the document contains 19,971 words. A renewed request to file an oversized brief is pending before this Honorable Court.

2. This document complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because the document has been prepared in a proportionally spaced typeface using Microsoft Word 2016 in Times New Roman, 14-point font.

/s/ Maksim Nemtsev
Maksim Nemtsev

CERTIFICATE OF SERVICE

I, Maksim Nemtsev, hereby certify that on March 25, 2024, this Brief and the Joint Appendix was filed with the Court through its CM/ECF system, thus effectuating service on all parties to this appeal.

/s/ Maksim Nemtsev
Maksim Nemtsev

ADDENDUM

TABLE OF CONTENTS

Caption **Page**

AO 245B (Rev. 02/18) Judgment in a Criminal Case
Sheet 1

UNITED STATES DISTRICT COURT

District of Massachusetts

UNITED STATES OF AMERICA
v.
Vladislav Klyushin

JUDGMENT IN A CRIMINAL CASE

Case Number: 1: 21 CR 10104 - PBS - 01

USM Number: 79306-509

Maksim Nemtsev
Defendant's Attorney

THE DEFENDANT:

☐ pleaded guilty to count(s) _____

☐ pleaded nolo contendere to count(s) _____
which was accepted by the court.

☑ was found guilty on count(s) 1-4
after a plea of not guilty.

The defendant is adjudicated guilty of these offenses:

Title & Section	Nature of Offense	Offense Ended	Count
18 USC § 371	Conspiracy to Obtain Unauthorized Access to Computer, and to Commit Wire Fraud & Securities Fraud	09/30/20	1
18 USC § 1343	Wire Fraud	10/24/18	2
18 USC § 1030(a)(4)	Unauthorized Access to Computers	10/24/18	3
15 USC § 78j(b)78ff(a)	Securities Fraud	01/23/20	4

The defendant is sentenced as provided in pages 2 through 5 of this judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

☐ The defendant has been found not guilty on count(s) _____

☐ Count(s) _____ ☐ is ☐ are dismissed on the motion of the United States.

It is ordered that the defendant must notify the United States attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this judgment are fully paid. If ordered to pay restitution, the defendant must notify the court and United States attorney of material changes in economic circumstances.

9/7/2023
Date of Imposition of Judgment

Signature of Judge

The Honorable Patti B. Saris
Judge, U.S. District Court
Name and Title of Judge

9/11/23
Date

AO 245B (Rev.02/18) Judgment in Criminal Case
Sheet 2 — Imprisonment

DEFENDANT: Vladislav Klyushin
CASE NUMBER: 1: 21 CR 10104 - PBS - 01

IMPRISONMENT

The defendant is hereby committed to the custody of the Federal Bureau of Prisons to be imprisoned for a total term of: 9 years

This term includes a term of 5 years on Counts 1 and 3, and terms of 9 years on Counts 2 and 4, to be served concurrently.

☑ The court makes the following recommendations to the Bureau of Prisons:

CREDIT FOR TIME SERVED; THAT THE DEFENDANT SERVED HIS TIME AT FCI OTISVILLE, NY

☑ The defendant is remanded to the custody of the United States Marshal.

☐ The defendant shall surrender to the United States Marshal for this district:

☐ at _____ ☐ a.m. ☐ p.m. on _____.

☐ as notified by the United States Marshal.

☐ The defendant shall surrender for service of sentence at the institution designated by the Bureau of Prisons:

☐ before 2 p.m. on _____.

☐ as notified by the United States Marshal.

☐ as notified by the Probation or Pretrial Services Office.

RETURN

I have executed this judgment as follows:

Defendant delivered on _____ to _____

a _____, with a certified copy of this judgment.

_____
UNITED STATES MARSHAL

By _____
DEPUTY UNITED STATES MARSHAL

DEFENDANT: Vladislav Klyushin
CASE NUMBER: 1: 21 CR 10104 - PBS - 01

SUPERVISED RELEASE

Upon release from imprisonment, you will be on supervised release for a term of : month(s)

NO TERM OF SUPERVISION IMPOSED.

MANDATORY CONDITIONS

1. You must not commit another federal, state or local crime.
2. You must not unlawfully possess a controlled substance.
3. You must refrain from any unlawful use of a controlled substance. You must submit to one drug test within 15 days of release from imprisonment and at least two periodic drug tests thereafter, as determined by the court.
   - ☐ The above drug testing condition is suspended, based on the court's determination that you pose a low risk of future substance abuse. *(check if applicable)*
4. ☐ You must cooperate in the collection of DNA as directed by the probation officer. *(check if applicable)*
5. ☐ You must comply with the requirements of the Sex Offender Registration and Notification Act (34 U.S.C. § 20901, *et seq.*) as directed by the probation officer, the Bureau of Prisons, or any state sex offender registration agency in the location where you reside, work, are a student, or were convicted of a qualifying offense. *(check if applicable)*
6. ☐ You must participate in an approved program for domestic violence. *(check if applicable)*

You must comply with the standard conditions that have been adopted by this court as well as with any other conditions on the attached page.

AO 245B (Rev. 02/18) Judgment in a Criminal Case
Sheet 5 — Criminal Monetary Penalties

DEFENDANT: Vladislav Klyushin
CASE NUMBER: 1: 21 CR 10104 - PBS - 01

CRIMINAL MONETARY PENALTIES

The defendant must pay the total criminal monetary penalties under the schedule of payments on Sheet 6.

	Assessment	JVTA Assessment*	Fine	Restitution
TOTALS	$ 400.00	$	$	$

☑ The determination of restitution is deferred until 12/5/2023. An *Amended Judgment in a Criminal Case (AO 245C)* will be entered after such determination.

☐ The defendant must make restitution (including community restitution) to the following payees in the amount listed below.

If the defendant makes a partial payment, each payee shall receive an approximately proportioned payment, unless specified otherwise in the priority order or percentage payment column below. However, pursuant to 18 U.S.C. § 3664(i), all nonfederal victims must be paid before the United States is paid.

Name of Payee	Total Loss**	Restitution Ordered	Priority or Percentage
TOTALS	$ 0.00	$ 0.00	

☐ Restitution amount ordered pursuant to plea agreement $ _____

☐ The defendant must pay interest on restitution and a fine of more than $2,500, unless the restitution or fine is paid in full before the fifteenth day after the date of the judgment, pursuant to 18 U.S.C. § 3612(f). All of the payment options on Sheet 6 may be subject to penalties for delinquency and default, pursuant to 18 U.S.C. § 3612(g).

☐ The court determined that the defendant does not have the ability to pay interest and it is ordered that:

☐ the interest requirement is waived for the ☐ fine ☐ restitution.

☐ the interest requirement for the ☐ fine ☐ restitution is modified as follows:

* Justice for Victims of Trafficking Act of 2015, Pub. L. No. 114-22.
** Findings for the total amount of losses are required under Chapters 109A, 110, 110A, and 113A of Title 18 for offenses committed on or after September 13, 1994, but before April 23, 1996.

DEFENDANT: Vladislav Klyushin
CASE NUMBER: 1: 21 CR 10104 - PBS - 01

SCHEDULE OF PAYMENTS

Having assessed the defendant's ability to pay, payment of the total criminal monetary penalties is due as follows:

A ☑ Lump sum payment of $ 400.00 due immediately, balance due

☐ not later than _____, or
☐ in accordance with ☐ C, ☐ D, ☐ E, or ☐ F below; or

B ☐ Payment to begin immediately (may be combined with ☐ C, ☐ D, or ☐ F below); or

C ☐ Payment in equal _____ *(e.g., weekly, monthly, quarterly)* installments of $ _____ over a period of _____ *(e.g., months or years)*, to commence _____ *(e.g., 30 or 60 days)* after the date of this judgment; or

D ☐ Payment in equal _____ *(e.g., weekly, monthly, quarterly)* installments of $ _____ over a period of _____ *(e.g., months or years)*, to commence _____ *(e.g., 30 or 60 days)* after release from imprisonment to a term of supervision; or

E ☐ Payment during the term of supervised release will commence within _____ *(e.g., 30 or 60 days)* after release from imprisonment. The court will set the payment plan based on an assessment of the defendant's ability to pay at that time; or

F ☐ Special instructions regarding the payment of criminal monetary penalties:

Unless the court has expressly ordered otherwise, if this judgment imposes imprisonment, payment of criminal monetary penalties is due during the period of imprisonment. All criminal monetary penalties, except those payments made through the Federal Bureau of Prisons' Inmate Financial Responsibility Program, are made to the clerk of the court.

The defendant shall receive credit for all payments previously made toward any criminal monetary penalties imposed.

☐ Joint and Several

Defendant and Co-Defendant Names and Case Numbers *(including defendant number)*, Total Amount, Joint and Several Amount, and corresponding payee, if appropriate.

☐ The defendant shall pay the cost of prosecution.

☐ The defendant shall pay the following court cost(s):

☑ The defendant shall forfeit the defendant's interest in the following property to the United States:

See Order of Forfeiture

Payments shall be applied in the following order: (1) assessment, (2) restitution principal, (3) restitution interest, (4) fine principal, (5) fine interest, (6) community restitution, (7) JVTA assessment, (8) penalties, and (9) costs, including cost of prosecution and court costs.

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	Criminal Action
v.	)	No. 21-10104-PBS
	)	
VLADISLAV KLYUSHIN,	)	
	)	
Defendant.	)	

MEMORANDUM AND ORDER

December 2, 2022

Saris, D.J.

INTRODUCTION

A grand jury indicted Russian national Vladislav Klyushin for allegedly hacking into American computer systems and using the confidential information he obtained to make profitable trades in the shares of public companies. The Indictment states four counts against Klyushin and his alleged co-conspirators Ivan Ermakov and Nikolai Rumiantcev: (I) Conspiracy, (II) Wire Fraud, (III) Unauthorized Access to Computers, and (IV) Securities Fraud. Klyushin now moves to dismiss Count IV of the Indictment and to partially dismiss Count I as to the allegations of conspiracy to commit securities fraud. Klyushin further asks the Court to suppress evidence the government seized pursuant to search warrants. After hearing, the Court **DENIES** the motion to dismiss and **DENIES** the motion to suppress.

FACTUAL BACKGROUND

A. The Indictment

The Indictment alleges the following facts.

Klyushin was the owner and first deputy general director of M-13, a purported information technology company in Moscow. Ermakov and Rumiantcev were deputy general directors of M-13. M-13 offered technological and media monitoring services to enterprises and government entities in Russia, including testing and analyzing organizations' cybersecurity preparedness. M-13 also offered investment management services to at least three individuals in exchange for up to 60 percent of the profits.

From approximately January 2018 through September 2020, Klyushin, Ermakov, and Rumiantcev schemed to gain access to information stored on the computer networks of two American filing agents ("Filing Agent 1" and "Filing Agent 2"), then traded on the information for profit. Filing agents assist public companies with their SEC filings. Consequently, they frequently possess the quarterly and annual financial data of public companies before they become public. Klyushin, Ermakov, Rumiantcev, and their co-conspirators operated malicious software to steal the usernames and passwords of employees of Filing Agents 1 and 2, and then used the credentials to log into the Filing Agents' computer networks. Once inside the Filing Agents' networks, the defendants and their co-conspirators viewed or downloaded the financial disclosures of

publicly traded companies and used the data to make profitable trades on securities exchanges.

On January 21, 2020, Ermakov used the login credentials of an employee of Filing Agent 1 to access the quarterly earnings information of Avnet, Inc., whose securities trade on the NASDAQ. Two days later, Ermakov used Klyushin's account at a Denmark-based bank to take a short position in Avnet securities, betting that their value would fall. Another co-conspirator also shorted Avnet shares. Hours after these trades, Avnet reported disappointing quarterly financial results.

The Indictment recites additional specific examples of the co-conspirators using employee login credentials to access the Filing Agents' computer networks and trading on public company financial information they found.

B. The Search Warrants

The government seized evidence pursuant to a search warrant directed to Apple, Inc. on September 29, 2020 (the "September 29 Search Warrant") and search warrants directed to Apple, Inc. and Google, LLC on October 13, 2020 (the "October 13 Search Warrants"). The government based its search warrant applications on two affidavits of FBI Special Agent BJ Kang (the "September 29 Affidavit" and the "October 13 Affidavit"). In the September 29 Affidavit, the government sought to search the email address MIKKA777@yahoo.com, belonging to another target of the

investigation, Mikhail Irzak, and Klyushin's Apple iCloud account associated with the email address 9227748@gmail.com. The October 13 Affidavit was in support of applications to search the Apple iCloud account associated with the Apple ID 1093366326 and the Google account 9227748@gmail.com, both linked to Klyushin. The two affidavits are substantially similar, and the Court will recite the facts they aver while noting any material differences.

The affidavits discuss the allegedly unlawful trading activities of various of the targets, focusing on Irzak and Klyushin. In September 2019, the SEC informed the FBI that it had identified a group of traders, including Irzak, who had made suspicious trades in the shares of several publicly traded companies before their earnings announcements. Approximately 95% of the companies whose shares the traders purchased or sold used Filing Agent 1 or Filing Agent 2 to assist with their quarterly filings. On January 16, 2020, the Financial Industry Regulatory Authority notified the SEC that in October and November, 2019, a client account at Otkritie Broker, Ltd., a Cyprus-based brokerage firm headquartered in Russia, had made profitable trades in the immediate leadup to 21 quarterly earnings announcements. Irzak traded in parallel with many of this account's trades. In early 2020, the FBI learned that Filing Agent 1 and 2's computer networks and employee login credentials were compromised. Through the

Filing Agent 1 hack, Avnet's earnings data was exposed on January 21, 2020.

The affidavits tie Klyushin to the scheme through Ermakov's Avnet trades. Ermakov had been indicted in the District of Columbia for interference in the 2016 United States elections and in the Western District of Pennsylvania for hacking into the servers of various sporting and anti-doping agencies. Special Agent Kang's review of Ermakov's Apple account showed that Ermakov had access to an account belonging to Klyushin on the SaxoTraderGO app[1] and that the account had images of Avnet "contracts for difference" dated January 23, 2020.[2] Irzak and other overseas traders sold Avnet shares short on the same day. The September 29 Affidavit (but not the October 13 Affidavit) also states that Klyushin's Saxo trading account "is believed to have traded in parallel with IRZAK in multiple publicly traded companies generally within hours of earning's announcements." Dkt. 98 ¶ 38. At the hearing, the government could not explain why the statement was struck from the October 13 Affidavit.

Special Agent Kang found that Ermakov listed Klyushin's phone

[1] The app is a mobile trading platform for Saxo Bank clients. The September 29 Affidavit describes Saxo Bank as "a Danish-based investment bank that specializes in online trading and investment." Dkt. 98 ¶ 29.

[2] A contract for difference is an agreement that allows traders to speculate as to the future movement of a stock price.

as a contact. He also learned that Klyushin was associated with the 9227748@gmail.com address and that Ermakov and Klyushin had corresponded over WhatsApp on many occasions between May 29, 2020 and July 9, 2020. Ermakov had an entry on his Apple calendar that indicated he had a meeting with "Vlad" about the stock exchange. Dkt. 98 ¶ 40; Dkt. 98-2 ¶ 25. Special Agent Kang believed the "Vlad" may have been a reference to Klyushin.

The Magistrate Judge issued the September 29 Search Warrant authorizing the FBI to search Klyushin's Apple iCloud account associated with the email address 9227748@gmail.com. Review of the Apple-produced records showed that this account was locked but that Klyushin's phone was associated with the Apple ID 1093366326. Accordingly, the FBI submitted the October 13 Affidavit. The Magistrate Judge issued the October 13 Search Warrants, which authorized the FBI to search both the iCloud account with the Apple ID 1093366326 and the 9227748@gmail.com Google account. The warrant to Apple listed 19 categories of evidence as examples of the types of information the FBI could search and seize pursuant to the warrant.

DISCUSSION

A. Motion to Dismiss[3]

Klyushin seeks dismissal of Count IV of the Indictment,

[3] The Court denied the motion to dismiss at the October 31, 2022 hearing, and elaborates upon its reasoning for the denial below.

alleging securities fraud, and so much of Count I as alleges a conspiracy to commit securities fraud. An indictment "must be a plain, concise, and definite written statement of the essential facts constituting the offense charged." Fed. R. Crim. P. 7(c)(1). The Court presumes that the allegations of the indictment are true in assessing a motion to dismiss. See United States v. Dunbar, 367 F. Supp. 2d 59, 60 (D. Mass. 2005).

Count IV of the Indictment alleges that Klyushin violated Section 10(b) of the Securities Exchange Act of 1934 and the SEC's Rule 10b-5. These two provisions prohibit fraud in the purchase or sale of securities. Section 10(b) makes it unlawful

> for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce or of the mails, or of any facility of any national securities exchange . . . [t]o use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered . . . any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors.

15 U.S.C. § 78j(b).

Rule 10b-5 is the primary implementing regulation of Section 10(b), and makes it unlawful, in connection with the purchase or sale of any security,

> for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange, (a) To employ any device, scheme, or artifice to defraud, (b) To make any untrue statement of a material fact or to omit to state a material fact

> necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or (c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person.

17 C.F.R. § 240.10b-5.

The question before the Court is whether a hack-and-trade scheme like that alleged in the Indictment amounts to securities fraud. The parties agree that the Second Circuit is the only court of appeals to have addressed this question. Its holdings directly support the government's position that hacking into computer systems to obtain and trade on material, nonpublic information ("MNPI") is securities fraud. See S.E.C. v. Dorozhko, 574 F.3d 42, 50–51 (2d Cir. 2009); see also United States v. Khalupsky, 5 F.4th 279, 290–91 (2d Cir. 2021), cert. denied sub nom. Korchevsky v. United States, 142 S. Ct. 761 (2022).

Klyushin argues that he cannot be liable for securities fraud because he did not have a fiduciary duty to the companies he took information from or those whose securities he traded in. Dorozhko and Khalupsky squarely reject this argument's application in the context of a hack-and-trade scheme. See Dorozhko, 574 F.3d at 49 ("Even if a person does not have a fiduciary duty to disclose or abstain from trading, there is nonetheless an affirmative obligation in commercial dealings not to mislead.") (internal quotation marks omitted); Khalupsky, 5 F.4th at 290 ("Although a fiduciary duty is relevant to other securities violations -- e.g.,

insider trading -- it need not be shown to prove the securities fraud charged here: fraudulent trading in securities by an outsider."). Consistent with this caselaw, this Court holds that affirmatively misrepresenting one's identity to access, steal, and trade on confidential information is deceptive within the meaning of Section 10(b) and Rule 10b-5. Klyushin's motion to dismiss is therefore denied.

B. Motion to Suppress[4]

1. Probable Cause

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. In reviewing a probable cause determination, the Court gives "significant deference to the magistrate judge's initial evaluation" and reverses only if there is "no 'substantial basis' for concluding that probable cause existed." United States v. Ribeiro, 397 F.3d 43, 48 (1st Cir. 2005) (quoting United States v. Feliz, 182 F.3d 82, 86 (1st Cir. 1999)). "A warrant application must establish probable cause to believe that (1) a crime has been committed --

[4] The government represents that it does not intend to admit evidence from the Google account 9227748@gmail.com. The Court will deny as moot Klyushin's motion to suppress evidence obtained from that account. The Court's suppression analysis concerns Klyushin's Apple accounts.

the 'commission' element, and (2) enumerated evidence of the offense will be found at the place to be searched -- the so-called 'nexus' element." United States v. Bregu, 948 F.3d 408, 414 (1st Cir. 2020) (cleaned up). Assessing whether an affidavit supports a finding of probable cause requires making a "practical, common-sense decision whether, given all the circumstances set forth in the affidavit" there is "a fair probability that contraband or evidence of a crime will be found in a particular place." United States v. Tanguay, 787 F.3d 44, 50 (1st Cir. 2015) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

Here, there was probable cause for the warrants to search Klyushin's Apple accounts. Special Agent Kang's affidavits connect the dots from Irzak to Ermakov to Klyushin, showing that there was a fair probability that evidence of a hack-and-trade scheme would be found in Klyushin's iCloud account. See United States v. Adams, 971 F.3d 22, 32 (1st Cir. 2020). The affidavits show that (1) there was an ongoing scheme, in which Irzak participated, that involved hacking into the Filing Agents' computer networks to obtain and trade on MNPI, including Avnet's MNPI; (2) Ermakov, a known hacker, had also traded in Avnet on the day of its earnings announcement; and (3) Ermakov had used Klyushin's account to make the Avnet trades and had corresponded with Klyushin repeatedly via phone in the months after the Avnet trades. A commonsense evaluation of these facts indicates that a

fair probability existed that Klyushin's iCloud account would contain evidence of the Avnet trades as part of the hack-and-trade scheme. Once the fruits of the September 29 Search Warrant showed that Klyushin's initial iCloud account was locked but that his phone was associated with the Apple ID 1093366326, there was also probable cause to search that second iCloud account.

Klyushin argues that the affidavits do not adequately tie him to a broad hack-and-trade scheme. He takes particular issue with Special Agent Kang's statement in the September 29 Affidavit that Klyushin's Saxo trading account "is believed to have traded in parallel with IRZAK in multiple publicly traded companies generally within hours of earning's announcements." Dkt. 98 ¶ 38. The Court agrees that this statement is too vague (who "believed" it? On what basis?) to support a finding of probable cause. See United States v. Vigeant, 176 F.3d 565, 571 (1st Cir. 1999) (holding that "unsupported conclusions are not entitled to any weight in the probable cause determination."). Nonetheless, the Court finds that the other supported assertions in the affidavits, and particularly Ermakov's use of Klyushin's account to trade in Avnet shares in parallel with Irzak, suffice to establish probable cause to search Klyushin's iCloud accounts for evidence of the hack-and-trade scheme.

Even if there were no probable cause, suppression is unwarranted because the good faith exception to the exclusionary

rule would apply. Under the good faith exception, the government may use evidence obtained pursuant to a later-invalidated warrant if it acted with objective good faith based on a probable cause determination issued by a neutral and detached magistrate. See United States v. Leon, 468 U.S. 897, 920 (1984). The First Circuit has delineated the boundaries of the good-faith exception:

> Suppression remains appropriate:
> 1. If the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth.
> 2. Where the issuing magistrate wholly abandoned his judicial role.
> 3. Where the executing officer relies on a warrant based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.

United States v. Levin, 874 F.3d 316, 322 (1st Cir. 2017) (internal punctuation omitted) (quoting Leon, 468 U.S. at 923).

The government proffers that Special Agent Kang believed that Klyushin's account had traded in parallel with Irzak because the SEC sent him a spreadsheet evidencing such parallel trades. While the spreadsheet is not incorporated into the affidavits and does not bear on the probable cause analysis, it is relevant to Special Agent Kang's good faith. Thus, even if (contrary to the Court's finding) there were no probable cause for the search warrants, the good faith exception would apply and suppression would be inappropriate.

2. Particularity

To satisfy the Fourth Amendment's particularity requirement, a warrant "(1) must supply enough information to guide and control the executing agent's judgment in selecting where to search and what to seize, and (2) cannot be too broad in the sense that it includes items that should not be seized." United States v. Kuc, 737 F.3d 129, 133 (1st Cir. 2013). The purpose of this requirement is "to prevent wide-ranging general searches by the police." United States v. Moss, 936 F.3d 52, 58 (1st Cir. 2019) (quoting United States v. Bonner, 808 F.3d 864, 866 (1st Cir. 1986)). A court must review the warrant's language as a whole in determining whether the warrant satisfies the particularity requirement. See Kuc, 737 F.3d at 133.

The warrants in this case each authorize law enforcement to search and seize information for the period January 1, 2018 to the time of search that constitute evidence of six offenses: wire fraud, conspiracy to commit wire fraud, fraud and related activity in connection with computers, money laundering and conspiracy to commit money laundering, securities fraud, and conspiracy to commit securities fraud. The Apple warrants then list nineteen examples of records that are among the types of evidence the government may search and seize. These categories include information related to MNPI of public companies; any relationship between the alleged participants in the scheme, including Irzak,

Klyushin, and Ermakov; Saxo Bank and other banks; intrusions into public networks; and filing agents for public companies. Other courts in this district have held that this structure satisfies the particularity requirement. See, e.g., United States v. Kanodia, No. 15-cr-10131-NMG, 2016 WL 3166370, at *5 (D. Mass. June 6, 2016); United States v. Tsarnaev, 53 F. Supp. 3d 450, 456–57 (D. Mass. 2014).

Klyushin argues that the warrants are overbroad because they (1) use non-exhaustive prefatory language describing the offenses at issue and the examples of documents to be seized, and (2) authorize the search of his iCloud account, which contains huge amounts of personal and irrelevant information. Even if the nineteen categories are broadly phrased, the language of the paragraphs must be read in context of the crimes at issue. See Kuc, 737 F.3d at 133–34. Indeed, a warrant need only provide reasonable specificity as to the categories of documents to be searched. See Archer v. Chisholm, 870 F.3d 603, 616 (7th Cir. 2017) ("[The investigating officer] could not know *ex ante*, with pinpoint specificity, what documents and e-mails existed.").

It is true that the search warrants directed Apple to broadly turn over to the government an iCloud account that contained substantial details of Klyushin's personal life that went beyond the temporal and substantive scope of the categories in the search warrants. However, the warrants only authorized the government to

search for specific categories of information from that seized account.[5] The fact that the government was authorized to search an iCloud account produced by Apple does not violate the Fourth Amendment so long as the search is consistent with the warrant. See Fed. R. Crim. P. 41(e)(2)(B).

"Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." Riley v. California, 573 U.S. 373, 393, 397 (2014) (noting that "[o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity."). That a digital seizure of such immense storage capacity will reveal files containing irrelevant information is hardly novel, however, as "traditional searches for paper records, like searches for electronic records, have always entailed the exposure of records that are not the objects of the search to at least superficial examination in order to identify and seize those records that are." United States v. Ulbricht, 858 F.3d 71, 100 (2d Cir. 2017), abrogated on other grounds by Carpenter v. United States, 138 S. Ct. 2206 (2018). Here, it suffices that the warrants direct law enforcement to particular places to be searched (i.e., Klyushin's iCloud accounts), the time period of the

[5] In this context, the seizure of the documents from Apple came first, and the search second.

documents to be searched, the offenses at issue, and the nineteen examples of records to be searched.

Klyushin complains bitterly that the government seized and used personal information that falls outside the warrant's scope, for example, at the bail hearing. One magistrate judge has required that a cloud storage provider like Apple conduct some degree of pre-production triage to filter out irrelevant documents. See In re. Search of Info. Associated with [redacted]@mac.com, 25 F. Supp. 3d 1, 8 (D.D.C. 2014). The government has sometimes used its own filtration teams to weed out privileged materials. See United States v. Aboshady, 951 F.3d 1, 5 (1st Cir. 2020) (authorizing Google to turn over an entire Gmail account, followed by a filtration team review and then review by the investigative team). Both of these procedures make sense. However, Klyushin does not argue that these procedures are constitutionally required, and no cited caselaw supports such a requirement. See United States v. Taylor, 764 F. Supp. 2d 230, 237 (D. Me. 2011) (holding that the Fourth Amendment does not require the government to delegate a pre-screening function to the internet service provider). In any case, the remedy for an improper use of documents beyond the scope of the categories would be partial suppression of the unwarranted documents, not blanket suppression. See Aboshady, 951 F.3d at 9. Moreover, the

government has agreed not to use any documents prior to 2018 at trial.

3. Franks Hearing

An affidavit in support of probable cause is presumed valid. See Franks v. Delaware, 438 U.S. 154, 171 (1978). To obtain a hearing into an affiant's credibility, the defendant must make "a substantial preliminary showing that both (1) a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit and (2) the allegedly false statement is necessary to the finding of probable cause." United States v. Reiner, 500 F.3d 10, 14 (1st Cir. 2007) (cleaned up). An omission of information may also trigger a Franks hearing where the information is material. See United States v. Castillo, 287 F.3d 21, 25 (1st Cir. 2002). Where the defendant makes allegations that the affiant made a knowing or reckless falsehood, "those allegations must be accompanied by an offer of proof." Franks, 438 U.S. at 171.

Klyushin seeks a Franks hearing because the affidavits in support of probable cause did not disclose that a federal judge had cast doubt on Special Agent Kang's credibility in a previous insider trading case. Judge Holwell of the Southern District of New York found that Special Agent Kang made "misleading" and "literally false" statements in an affidavit in support of probable cause. United States v. Rajaratnam, No. 09-cr-1184, 2010 WL

4867402, at *10 (S.D.N.Y. Nov. 24, 2010). The affidavit failed to note that a cooperating witness had pleaded guilty to participating in a different insider trading scheme six years earlier -- a fact that could have cast doubt on the witness's credibility. See id. Moreover, the government had tried and failed in the same earlier case to establish insider trading by the defendant Rajaratnam, suggesting that it had been investigating him for years before the affidavit disclosed. See id. The court additionally found that Special Agent Kang had paraphrased certain phone conversations inaccurately. See id. at *10-*11. Finally, Judge Holwell faulted the government for failing to divulge that its criminal investigation had substantially relied on an SEC insider trading investigation into Rajaratnam, calling into question whether the wiretap at issue was necessary. See id. at *1. The court ordered a Franks hearing that only concerned whether the wiretap was necessary given the government's "reckless[]" failure to disclose the SEC investigation, but ultimately declined to suppress evidence after finding the omission immaterial. Id. at *1. On appeal, the Second Circuit reversed much of the district court's rulings on the falsity of Special Agent Kang's affidavit, finding that his omission of evidence regarding the SEC investigation had not occurred with "reckless disregard for the truth" and thus was not improper. United States v. Rajaratnam, 719 F.3d 139, 154-56 (2d Cir. 2013).

Here, binding precedent forecloses the possibility of a Franks hearing. In United States v. Southard, the First Circuit rejected the argument that a Franks hearing was warranted only because the district court had, in a prior related case, suppressed evidence following a Franks hearing arising from the same F.B.I. agent's affidavit. See 700 F.2d 1, 9-10 (1st Cir. 1983) (finding previous Franks hearing outcome "casts a certain degree of doubt upon" the affiant's credibility but nonetheless "proves nothing about the veracity of the affidavit at issue in this case and standing alone cannot establish appellants' right to a Franks hearing.").

Klyushin's argument in support of a Franks hearing relies entirely on the omission of Judge Holwell's critical statements - - which did not even result in the suppression of evidence in the Rajaratnam case. Without more, Klyushin is not entitled to a Franks hearing. Klyushin also has not shown how the alleged omission negates the Magistrate Judge's probable cause finding. He argues that it discredits Special Agent Kang's statement in the September 29 Affidavit that Klyushin's account was believed to have traded "in parallel" with Irzak. While the reason for the later omission of that assertion is unclear, the statement was not necessary to a finding of probable cause. Moreover, in light of the information from the SEC, there is no

reasonable inference of bad faith. Thus, Klyushin is not entitled to a Franks hearing.

ORDER

For the foregoing reasons, Klyushin's Motion to Dismiss (Dkt. 96) and Motion to Suppress (Dkt. 97) are **DENIED**.

SO ORDERED.

/s/ PATTI B. SARIS
Hon. Patti B. Saris
United States District Judge

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
v.	)	Criminal Action
	)	No. 21-10104-PBS
VLADISLAV KLYUSHIN,	)	
Defendant.	)	

MEMORANDUM AND ORDER

July 26, 2023

Saris, D.J.

INTRODUCTION

Following a 10-day trial, a jury convicted Vladislav Klyushin, a Russian national, of conspiring with Russian co-conspirators to hack into the computer systems of two American filing agents, Toppan Merrill and Donnelly Financial ("DFIN"), and use confidential information to make profitable trades in the American stock market. Specifically, the jury found him guilty of a conspiracy to obtain unauthorized access to computers or to commit wire fraud or securities fraud in violation of 18 U.S.C. § 371 (Count I); wire fraud in violation of 18 U.S.C. §§ 1343 & 2 (Count II); unauthorized access to computers in violation of 18 U.S.C. §§ 1030(a)(4) & 2 (Count III); and securities fraud in violation of 15 U.S.C. §§ 78j(b) & 78ff(a), 17 C.F.R. § 240.10b-5, and 18 U.S.C. § 2 (Count IV). The jury was instructed that to

convict, it had to also find that the government had proven by a preponderance of the evidence that for each count, this Court had venue.

Klyushin now moves for a judgment of acquittal under Fed. R. Crim. P. 29(c) for improper venue. Dkt. 222. He raises four main arguments. First, he argues that venue in this district was not foreseeable. Second, he argues that even if a Boston server was used to gain unauthorized access to confidential information, the hacked information comprised "packets of information" that passed through the server, and "pass through" venue is not proper in this case. Third, he argues no "essential conduct" of the crime occurred in the District of Massachusetts. Fourth, he argues that venue under 18 U.S.C. § 3238 for the conspiracy charge was improper. After hearing, the Court **DENIES** the motion to acquit.

FACTUAL BACKGROUND

Taken in the light most favorable to the government, the evidence supports the following facts relevant to the dispute on venue:

Klyushin was the owner and first deputy general director of M-13, an information technology company in Moscow. Co-conspirators Ivan Ermakov and Nikolai Rumiantcev were employees of M-13. M-13 purported to offer technological and media monitoring services to enterprises and government entities in Russia.

From approximately January 2018 through September 2020,

Klyushin, Ermakov, Rumiantcev, and others -- all Russians -- conspired to gain access to information stored on the computer networks of two American filing agents, Toppan Merrill and DFIN. Filing agents assist public companies with their Securities and Exchange Commission (SEC) filings, including by preparing reports of quarterly and annual financial data. Between October and November 2018, Klyushin and his co-conspirators gained unauthorized access to DFIN's network in Illinois via a Boston server. Once inside the DFIN system, the hackers downloaded[1] back to a server in Boston the confidential earnings reports of many public companies, using the stolen user credentials of a DFIN employee.

The Internet Protocol ("IP") addresses through which the conspirators downloaded the material non-public information ("MNPI") belonged to an IP address block (the "104 IPs") assigned to Stackpath, a virtual private network ("VPN") service provider. See Dkt. 181 at 123:23-127:11 (government expert testifying that the 104 IPs "obtained access to and downloaded" documents from

[1] The dictionary meaning of "download" is "to copy (a program, file, etc.) from a central or remote computer system to a computer, mobile device, etc., now usually via the internet." Download, Oxford English Dictionary, www.oed.com/view/Entry/57256 (last visited July 25, 2023). Another dictionary similarly defines "download" as "to transfer (as information, a file, or software) from a usually large remote computer to the memory of another device (as a smaller computer)." Download, Merriam-Webster Unabridged Dictionary, www.unabridged.merriam-webster.com/unabridged/download (last visited July 25, 2023).

DFIN). VPN service providers offer subscribers a way "to maintain a degree of anonymity on the Internet." Dkt. 217 at 44:16-21; see also id. at 17:18-18:1 (Defendant's expert J. Michael Roberts testifying: "[Y]ou connect to the server, and your traffic is routed to that server. That new VPN server is now acting as your on-ramp to the Internet. So everywhere that that connection goes to from that point [is] going to appear to be coming from that server.").

Stackpath, operating through subsidiaries (e.g., Strong Technology) and vendors (e.g., Micfo), leased a server physically located in a data center on Summer Street in Boston. The 104 IPs were assigned to this computer server, beginning on May 30, 2018 and through 2019.

The earnings reports accessed through the Boston server included those of dozens of publicly traded companies. Klyushin and his co-conspirators placed their trades only after the confidential information was downloaded through the Boston server, and revised their positions following public announcements of those earnings. For example, confidential information pertaining to Tesla was downloaded to the Boston server at 5:18 a.m. on October 24, 2018. Later that morning, Klyushin bought Tesla stock. After the market closed that day and the earnings were publicly announced, the conspirators immediately sold their shares to great profit. While the amount of total profits is disputed, the

government alleges that Klyushin profited in the amount of at least $36 million, and the conspiracy as a whole made more than $90 million in profits.

Klyushin, who resides in Russia, was arrested in Switzerland while on a skiing trip, and was extradited to the United States and brought directly to Boston.

JURY INSTRUCTIONS

The Court gave the jury one omnibus instruction on venue:

> The Constitution and federal law require that a criminal defendant must be tried in the state or district in which the offense is committed. Where an offense spans multiple jurisdictions or where a crime consists of distinct parts which have different localities, the whole may be tried where any part can be proved to have been done. Continuing offenses that are committed in more than one district may be prosecuted in any district which such offense was begun, continued, or completed. A defendant must be charged in a district that has a meaningful connection to the allegations. To determine whether a meaningful connection exists, you must consider the nature of the crime alleged and identify the crime's essential conduct elements []. You must also consider the locations where the criminal acts were committed. The government must prove for each offense -- so each one of those counts we just went through -- that venue is proper in the District of Massachusetts.
>
> Unlike all of the other elements that we talked about -- remember I said "proof beyond a reasonable doubt" numerous times -- but unlike all the elements that I have previously described, the government has to prove venue by a preponderance of the evidence. That's a legal term, "preponderance of the evidence." That means, to establish venue by a preponderance of the evidence, the government must prove that the fact is more likely true than not true[].
>
> To establish venue in this district, the government need not prove that the crimes themselves were committed

> entirely in this district, or that the defendant himself was present here.
>
> I'm now going to focus you on conspiracy.
>
> With regard to the conspiracy charged in Count One, there's no requirement that the entire conspiracy took place here in Massachusetts, or that the agreement was formed here. But for you to return a guilty verdict on the conspiracy charge in Count One, the government must prove by a preponderance of the evidence that any overt act in furtherance of the agreement took place here in Massachusetts.
>
> Alternatively -- now, I just want you to focus only on the conspiracy count with respect to what I'm about to tell you. Alternatively, with respect to the conspiracy count only, the government has this alternative theory of venue. Under federal law, where an offense is begun or committed outside the jurisdiction of any particular state or district, venue for prosecution of the offense is established in the district where the defendant is arrested or is first brought. For venue to be established for the conspiracy count under this alternative theory, the government must prove that it is more likely true than not true that the offense was begun or committed outside of the United States, and that the defendant was first brought to the District of Massachusetts. The government must also prove that the essential conduct elements of the conspiracy took place outside of the United States.
>
> If the government fails to prove venue by a preponderance of the evidence with respect to any count, you must find the defendant not guilty of that count only. So for every single of these verdict slips, you also have to find not only that the government proved the elements beyond a reasonable doubt, but also that it proved venue by a preponderance of the evidence, more likely true than not true.

Dkt. 218 at 136:10-138:18.

The parties did not object to the Court's delivery of an omnibus instruction on venue. On the second day of jury deliberations, the foreperson came to the Court with the following question: "If venue was properly established for one of the charged

counts, does that necessarily mean that venue is proper for the other counts?" Dkt. 219 at 4:20-22. After consulting with the parties, the Court instructed the jury by way of written answer: "You have to decide venue count by count. See Page 38, Lines 23 through 25," incorporating the instruction that "[t]he government must prove for each offense that venue is proper in the District of Massachusetts." Id. at 6:9-10, 5:6-10.

LEGAL STANDARD

The Court "may set aside [a] verdict and enter an acquittal" under Fed. R. Crim. P. 29(c). In ruling on a motion for judgment of acquittal under Rule 29, the Court must "consider the evidence as a whole taken in the light most favorable to the [g]overnment." United States v. Smith, 680 F.2d 255, 259 (1st Cir. 1982). If the guilty verdict is supported by a "plausible rendition" of the record, the Court must not disturb it. United States v. Moran, 312 F.3d 480, 487 (1st Cir. 2002).

In assessing a Rule 29 motion, the Court "do[es] not weigh the evidence or make any credibility judgments, as those are left to the jury." United States v. Merlino, 592 F.3d 22, 29 (1st Cir. 2010). Instead, the Court must "examine the evidence -- direct and circumstantial -- as well as all plausible inferences drawn therefrom[.]" United States v. Meléndez-González, 892 F.3d 9, 17 (1st Cir. 2018) (quoting United States v. Wyatt, 561 F.3d 49, 54 (1st Cir. 2009)). Here, the Court must decide whether a rational

jury could have found that venue was proper in this district as to each individual count. United States v. Salinas, 373 F.3d 161, 163 (1st Cir. 2004).

DISCUSSION

I. Venue

The Venue Clause of Article III of the Constitution mandates that the trial of all crimes "shall be held in the State where the said Crimes shall have been committed." U.S. Const. art. III, § 2, cl. 3. The Venue Clause also includes an exception: the trial for crimes "not committed within any State . . . shall be at such Place or Places as the Congress may by Law have directed." Id. Similarly, the Vicinage Clause guarantees "the right to . . . an impartial jury of the State and district wherein the crime shall have been committed." U.S. Const. amend. VI; see generally Smith v. United States, 599 U.S. __, 143 S.Ct. 1594, 1602 n.4 (2023) (slip op., at 4).

Courts must analyze venue separately for each individual count of an indictment. Salinas, 373 F.3d at 163. "If the statute under which the defendant is charged contains a specific venue provision, that provision must be honored[.]" Id. at 164. Where an offense "span[s] multiple jurisdictions, or 'where a crime consists of distinct parts which have different localities[,] the whole may be tried where any part can be proved to have been done.'" United States v. Seward, 967 F.3d 57, 60 (1st Cir. 2020)

(quoting United States v. Rodriguez-Moreno, 526 U.S. 275, 281 (1999)).

In the absence of specific venue guidance and where an offense is not continuing, the "locus delicti must be determined from the nature of the crime alleged and the location of the act or acts constituting it." Salinas, 373 F.3d at 164 (quoting United States v. Anderson, 328 U.S. 699, 703 (1946)). In doing so, courts "identify the conduct constituting the offense (the nature of the crime) and then discern the location of the commission of the criminal acts." Rodriguez-Moreno, 526 U.S. at 279.

A trial may be held "where any part of a crime can be proved to have been done." Smith, 599 U.S. __, 143 S.Ct. at 1603 (slip op., at 6) (cleaned up). For example, a defendant charged with illegally shipping goods may be tried in any state through which the goods were illegally transported. Armour Packing Co. v. United States, 209 U.S. 56, 77 (1908). Though action verbs are helpful, "requiring the presence of an action verb to define the nature of the crime could sweep out conduct not enumerated by such action language but nonetheless essential to the offense." Seward, 967 F.3d at 61; see also United States v. Miller, 808 F.3d 607, 618 (2d Cir. 2015) ("[A] myopic focus on verbs can lead to overlooking important statutory language that communicates the 'nature of the crime alleged,' which is the core of the inquiry.").

II. Statutory Venue

The government relies on the following statutory provision for multidistrict offenses:

> [A]ny offense against the United States begun in one district and completed in another, or committed in more than one district, may be inquired of and prosecuted in any district in which such offense was <u>begun, continued, or completed</u>.
> Any offense involving the use of the mails, transportation in interstate or foreign commerce, or the importation of an object or person into the United States is a continuing offense and, except as otherwise expressly provided by enactment of Congress, may be inquired of and prosecuted in any district from, through, or into which such commerce, mail matter, or imported object or person moves.

18 U.S.C. § 3237(a) (emphasis added). "The classic example of a continuing offense is a conspiracy[.]" United States v. Yashar, 166 F.3d 873, 875 (7th Cir. 1999). It has long been held that "venue [is] proper so long as any act in furtherance of [a] conspiracy was committed in the district[.]" United States v. Uribe, 890 F.2d 554, 558 (1st Cir. 1989); see also United States v. Santiago, 83 F.3d 20, 25 (1st Cir. 1996) (finding a "single, overt act" was "itself sufficient to sustain venue" in a drug conspiracy case).

III. Foreseeability

Klyushin argues that the government failed to prove that any of the conspirators "purposely availed themselves of a Boston-based IP address" or could have reasonably foreseen that they were accessing confidential information via a Boston-based server.

Dkt. 222 at 3. According to Klyushin, the Boston 104 IP addresses used in the hacking scheme were assigned at random by the VPN service provider. See id.; Dkt. 228 at 3. Moreover, these IP addresses were only used to access DFIN's network from late October to early November in 2018 -- a small window of time in the overall charged conspiracy. In Klyushin's telling, the evidence shows that Boston was a mere "pass through" to Russia which Klyushin could not reasonably have foreseen.

To support a foreseeability requirement, Klyushin relies primarily on caselaw from the Second Circuit, which held that venue is proper in a district where "(1) the defendant intentionally or knowingly causes an act in furtherance of the charged offense to occur in the district of venue or (2) it is foreseeable that such an act would occur in the district of venue." United States v. Svoboda, 347 F.3d 471, 483 (2d Cir. 2003). While the First Circuit has not itself addressed such a foreseeability argument, several circuits have explicitly rejected adopting this foreseeability requirement for venue. See, e.g., United States v. Renteria, 903 F.3d 326, 333 (3d Cir. 2018) (declining to "adopt a reasonable foreseeability test to establish venue under § 3237(a)"); United States v. Gonzalez, 683 F.3d 1221, 1226 (9th Cir. 2012) (same); United States v. Castaneda, 315 F. App'x 564, 569 (6th Cir. 2009) (same); United States v. Johnson, 510 F.3d 521, 527 (4th Cir. 2007)

(declining to "engraft a mens rea requirement onto a venue provision that clearly does not have one").

Given the weight of the caselaw,[2] the Court declines to adopt the foreseeability requirement for venue under the Constitution. Even if there were a foreseeability requirement, the Court does not find persuasive the argument that no jury could reasonably find that a defendant (or co-conspirators) who commits a crime by employing a VPN service provider that uses random IP addresses nationwide in order to preserve anonymity could not reasonably foresee that venue would exist in a district where the assigned server was located.

IV. Pass Through

Klyushin's primary argument is that the use of IP addresses traced to Boston was "purely coincidental," and that none of the "essential conduct elements" of any of the charged counts occurred in this district. Relying heavily on a Department of Justice Manual

---

[2] The Second Circuit recently addressed the foreseeability requirement in United States v. Kirk Tang Yuk, 885 F.3d 57 (2d Cir. 2018): "It is also true that our seminal case in this regard, [Svoboda] identified a foreseeability requirement without extensive analysis. Nonetheless, we are bound to examine this factor in assessing whether the venue of these prosecutions was proper as to each defendant." Id. at 69 n.2. The Third Circuit also analyzed the origin and development of this foreseeability requirement, noting, "[s]ignificantly, however, neither Svoboda nor Kim nor Bezmalinovic actually explains why reasonable foreseeability is required to establish venue under the Constitution. Rather, the cases seem to derive the reasonable foreseeability test from a generous reading of prior Second Circuit precedent." Renteria, 903 F.3d at 331.

("DOJ Manual"), Klyushin argues that even though hacked information was downloaded to the Boston 104 IP addresses, venue was improper because the Boston server was a mere "pass through." The government argues that the DOJ Manual is not binding, is outdated, and is unsupported by the caselaw. While it is true the DOJ Manual does not create legal rights, see United States v. Busher, 817 F.2d 1409, 1411 (9th Cir. 1987), the Manual is helpful in framing the issues here, so I quote the relevant excerpt in full:

> Multidistrict offenses "may be . . . prosecuted in any district in which such offense was begun, continued, or completed." 18 U.S.C. § 3237(a). Note that only the "essential conduct elements" of a crime qualify. United States v. Rodriguez-Moreno, 526 U.S. 275, 280 (1999). For instance, section 1030(a)(2)(C) prohibits intentionally accessing a computer without or in excess of authorization, and thereby obtaining information from any protected computer. The two essential conduct elements in section 1030(a)(2)(C) are "accessing" a computer and "obtaining" information. Thus, it would seem logical that a crime under section 1030(a)(2)(C) is committed where the offender initiates access and where the information is obtained.
>
> The exact location of each event -- the "accessing" and the "obtaining" -- may not always be easily determined.
>
> EXAMPLE: An intruder located in California uses communications that pass through a router in Arizona to break into a network in Illinois and then uses those network connections to obtain information from a server in Kentucky.
>
> The intruder initiated access in California, and the router in Arizona enabled that access. Arguably, however, the intruder did not achieve access until reaching the network in Illinois. Of course, one could also argue that access did not occur until the intruder reached the server in Kentucky where the information was located. Likewise, one could argue that the intruder

obtained the information in Kentucky, or that he did not obtain the information until it reached him in the district where he was located, in this case, California.

This example illustrates an offense governed by 18 U.S.C. § 3237(a). Under any of the options discussed above, the appropriate venue would seem to include both of the endpoints -- that is, the district in which the offender is located (California) and the district in which the information is located (Kentucky). It is likely that venue is also proper at some, if not all, of the points in between, since venue may lie "in any district in which [a continuing] offense was begun, continued, or completed." 18 U.S.C. § 3237(a). Under this section, the "accessing" and "obtaining" arguably continued in Arizona and Illinois. Certainly, venue seems proper in Illinois where the intruder broke into the network. Whether the intruder committed a crime in Arizona is less clear.

Prosecutors looking to fix venue in the locale through which communications passed, as in the case of the router in Arizona, should look closely at the facts to determine whether venue in that district would satisfy the framework discussed above. The case for "pass through" venue may be stronger where transmission of the communications themselves constitutes the criminal offense (e.g., when a threatening email is sent in violation of 18 U.S.C. § 1030(a)(7)) and the path of transmission is certain (e.g., when an employee's email is sent through a company mail server in a particular state). . . . By contrast, in cases where the path of transmission is unpredictable, a court may find it difficult to conclude that a crime was committed in a district merely because packets of information happened to travel through that district. . . . Of course, where the "pass through" computer itself is attacked, venue would likely be proper based on the attack, without reference to pass-through rationale.

Federal prosecutors should also take note of the Department of Justice's policies for wire and mail fraud, which may be analogous. For wire fraud, section 967 of the Department's Criminal Resource Manual provides that prosecutions "may be instituted in any district in which an interstate or foreign transmission was issued or terminated." Crim. Resource Manual § 967. Although the text of section 967 refers only to the place of issuance or termination, the case cited in support of that proposition, United States v. Goldberg, 830 F.2d

> 459, 465 (3d Cir. 1987), relies on 18 U.S.C. § 3237(a), which also includes the place where the conduct continued, thus leaving open the door to "pass through" venue. In the case of mail fraud, section 9-43.300 of the U.S. Attorneys' Manual states that Department of Justice policy "opposes mail fraud venue based solely on the mail matter passing through a jurisdiction." USAM 9-43.300; see also Crim. Resource Manual § 966.

Comput. Crime & Intell. Prop. Section, Office of Legal Education, Prosecuting Computer Crimes, at 118-20, http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf (last visited July 25, 2023).

Analogizing the role of the Boston server in this case to that of the router in Arizona, Klyushin emphasizes the language that "where the path of transmission is unpredictable, a court may find it difficult to conclude that a crime was committed in a district merely because pockets of information happened to travel through that district." Dkt. 222 at 5.

To nail down his point, Klyushin relies on United States v. Auernheimer, 748 F.3d 525 (3d Cir. 2014), which provides a thoughtful discussion on venue in the cybercrime context:

> As we progress technologically, we must remain mindful that cybercrimes do not happen in some metaphysical location that justifies disregarding constitutional limits on venue. People and companies still exist in identifiable places in the physical world. When people commit crimes, we have the ability and obligation to ensure that they do not stand to account for those crimes in forums in which they performed no "essential conduct element" of the crimes charged.

Id. at 541 (emphasis added). The district court in Auernheimer found that venue was proper in New Jersey for charges of conspiracy to violate the Computer Fraud and Abuse Act and identity fraud because the unlawful disclosure of 4,500 New Jersey residents' email addresses affected New Jersey citizens. Id. at 531. In reversing, the Third Circuit distinguished "essential conduct elements," which can provide the basis for venue, from "circumstance elements," which cannot. Id. at 533 (citing to Rodriguez-Moreno, 526 U.S. at 280 n.4). The Third Circuit held that venue was improper in New Jersey because, as the accessed servers were located in Texas and Georgia and the conspirators were only ever located in California and Arkansas, "[n]o protected computer was accessed and no data was obtained in New Jersey." Id. at 534. Further, the Third Circuit found that none of the alleged overt acts that the government alleged in the indictment occurred in New Jersey. Id. at 535. In Auernheimer, the conspirators did not use an IP address on a server within New Jersey to access or obtain information remotely. Id. at 536.

Here, the government argues that Auernheimer is distinguishable because IP addresses on the Boston server in Massachusetts were used in accessing confidential information -- downloading and transmitting the information to Russia. Therefore, in the government's view, the essential conduct element of

accessing confidential information and obtaining it happened in Boston.

The parties have not cited any cases addressing venue where out-of-district actors caused in-district computers to perform the essential criminal acts. While it is a novel issue, the government has the better argument. The Supreme Court has declined to hold that "verbs are the sole consideration in identifying the conduct that constitutes an offense." Rodriguez-Moreno, 526 U.S. at 280. Moreover, in Smith, the Supreme Court cited favorably to an old case, Armour Packing, to support venue for a continuing crime in any district where the transportation of illegal goods occurred. 599 U.S. __, 143 S.Ct. at 1603 (slip op., at 6). In other contexts, courts addressing criminal convictions have found proper venue involving "pass through" intermediaries. See, e.g., United States v. Blecker, 657 F.2d 629, 633 (4th Cir. 1981) (finding proper venue for a false claims conviction "in either the district in which the false claim is submitted to the intermediary or the district in which the intermediary transmits the false claim to the agency"). While Klyushin hit send on a computer in Russia, given the nature of the charged continuing crimes, he caused the crimes to be implemented in part in Massachusetts. Based on this evidence concerning the use of a server in Boston, a jury could reasonably find by a preponderance of the evidence that Klyushin's use of the

IP addresses in Boston was essential conduct, and that Massachusetts had a meaningful connection to the crimes committed.

V. Section 3238

The government asserts venue under the so-called "High Seas" or "First Brought" venue provision, 18 U.S.C. § 3238. Section 3238 provides that the "trial of all offenses begun or committed upon the high seas, or elsewhere out of the jurisdiction of any particular State or district, shall be in the district in which the offender, or any one of two or more joint offenders, is arrested or is first brought[.]" 18 U.S.C. § 3238.

Relying on language in Article III, § 2, cl. 3 of the Constitution, Klyushin argues that § 3238 provides venue only for offenses "not committed within any State." Moreover, he contends that under the statute, venue is only proper where the offense was committed outside of any district, pointing to the section's title "Offenses not committed in any district" to support his contention. However, a title may not alter the plain meaning of the text. Miller, 808 F.3d at 619. The provision is not restricted to crimes "wholly" committed outside the United States. Id. The plain language of the statute permits trial of all offenses begun or committed outside of any state. See Chandler v. United States, 171 F.2d 921, 931-32 (1st Cir. 1948) (holding that the provision must be given its "broad literal meaning"). Klyushin's claim of

unconstitutionality is conclusory and not supported by any caselaw.

The fundamental question in deciding the application of § 3238 is whether the acts are "essentially foreign." See United States v. Pendleton, 658 F.3d 299, 304-05 (3d Cir. 2011) (holding that the crux of the defendant's offense was "committed" outside of the jurisdiction of any state or district, making the crime "essentially foreign"); Miller, 808 F.3d at 620 (holding that an offense occurred "in its essence" abroad was "essentially foreign," and venue could be established "even though certain offense conduct occurred in the United States").

VI. Sufficiency of Evidence on Each Count

With these legal principles in mind, the Court addresses each count.

A. Conspiracy (Count I)

A rational jury could find that an overt act in furtherance of the conspiracy took place in Boston as charged in the indictment See Dkt. 8 at 7-8 (alleging that one of the conspirators "obtain[ed] unauthorized access to the computer network of [a filing agent] through an IP address hosted at a data center located in Boston, Massachusetts"). The government presented evidence that on or about October 22 and 24, 2018, one of the conspirators caused the username and password of a DFIN employee to be transmitted from the Boston server to DFIN's network, for the purpose of

obtaining unauthorized access, committing wire fraud, or committing securities fraud, and then causing the information to be transmitted to Russia.

A rational jury could have found that the conspiracy in Count I was "essentially foreign," as the conspiracy was complete (in Russia) at the time any overt act in furtherance of the conspiracy was committed. Therefore, venue was also sufficiently proven under 18 U.S.C. § 3238.

B. Wire Fraud (Count II)

Under 18 U.S.C. § 1343, the government must prove that a conspirator "knowingly and willfully participated in a scheme to defraud by means of false pretenses, and that he used interstate wire communications in furtherance of the scheme." United States v. Gorski, 880 F.3d 27, 37 (1st Cir. 2018).

Courts have held that wire fraud is considered a "continuing" offense under § 3237(a). United States v. Carpenter, 405 F. Supp. 2d 85, 91 (D. Mass. 2005), aff'd in part, appeal dismissed in part, 494 F.3d 13 (1st Cir. 2007) (holding that Massachusetts was an appropriate venue for a wire fraud transaction that began in New Hampshire, cleared through the Federal Reserve Bank in Boston, and continued to a Merrill Lynch account in Pennsylvania). "[V]enue is established in those locations where the wire transmission at issue originated, passed through, or was received, or from which it was 'orchestrated.'" United States v. Pace, 314 F.3d 344, 349 (9th Cir.

2002) (emphasis added); United States v. Goldberg, 830 F.2d 459, 465 (3d Cir. 1987) (finding that § 1343 is a "continuing offense crime[] pursuant to 18 U.S.C. § 3237"). "[T]o the extent a wire communication is sent from one district to or through one or more others . . . venue [is] proper in any district in which the offense was 'begun, continued, or completed.'" Carpenter, 405 F. Supp. 2d at 91 (emphases added).

A rational jury could find that a username and password were repeatedly transmitted over the Boston 104 IPs to DFIN's servers, to gain direct unauthorized access to the DFIN computer network, and that those wire communications continued through Boston. A rational jury could have therefore found venue in Massachusetts as to Count II.

C. Unauthorized Access to Computers (Count III)

A person violates the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(4), when he "[k]nowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value[.]" 18 U.S.C. § 1030(a)(4). The CFAA makes no reference to the venue of the offense and can therefore be prosecuted as a continuing offense under § 3237(a). See 18 U.S.C. § 3237(a) ("Any offense involving . . . transportation in interstate or foreign commerce . . . is a continuing offense"). Accessing without authorization and

obtaining confidential information have been held to be "essential conduct elements" of crimes under the CFAA. See Auernheimer, 748 F.3d at 533-34. As previously stated, there is sufficient evidence for a rational jury to find that the "downloading" of confidential information to the Boston server fulfills the essential conduct element of obtaining something of value.

D. Securities Fraud (Count IV)

Under the Securities Exchange Act of 1934, 15 U.S.C. § 78j(b), it is unlawful to "use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered, or any securities-based swap agreement, any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe[.]" The Act's venue provision states that a "criminal proceeding may be brought in the district wherein any act or transaction constituting the violation occurred." 15 U.S.C. § 78aa. The government argues that the use of a DFIN employee's password to access DFIN's network without authorization constituted a "deceptive device or contrivance" and occurred using the Boston 104 IPs. "A securities fraud violation occurs where defendants 'use or employ . . . any manipulative or deceptive device,' including the making of material false statements." United States v. Lange, 834 F.3d 58, 69 (2d Cir. 2016) (finding false statements communicated by wire into the district where the

crime was prosecuted were "crucial to the success of the scheme"). Venue has been held to be proper "not only in the district where telephonic or electronic materially fraudulent communications were initiated, but also in the district where such communications were received." Id. at 70.

A rational jury could find that the conspirators used stolen employee credentials to download confidential information onto a Boston server, and then used that information in the purchase and sale of securities. A rational jury thus had sufficient evidence to find that an "essential conduct element" of securities fraud occurred in Massachusetts under a preponderance standard.

ORDER

For the foregoing reasons, Klyushin's Motion to Acquit for Improper Venue (Dkt. 222) is **DENIED**.

SO ORDERED.

/s/ PATTI B. SARIS
Hon. Patti B. Saris
United States District Judge

also need not be central to the execution of the scheme. All that is required is that the use of any instrumentality of interstate commerce bear some relation to the object of the scheme or fraudulent conduct.

So I've now gone through all the elements of all counts, but let's stand and stretch because I've got to talk to you about venue, all right?

(Pause.)

THE COURT: Venue, what's venue? Please be seated.

02:10 The Constitution and federal law require that a criminal defendant must be tried in the state or district in which the offense is committed. Where an offense spans multiple jurisdictions or where a crime consists of distinct parts which have different localities, the whole may be tried where any part can be proved to have been done. Continuing offenses that are committed in more than one district may be prosecuted in any district which such offense was begun, continued, or completed. A defendant must be charged in a district that has a meaningful connection to the allegations. To determine

02:11 whether a meaningful connection exists, you must consider the nature of the crime alleged and identify the crime's essential conduct elements, essential conduct elements. You must also consider the locations where the criminal acts were committed. The government must prove for each offense -- so each one of those counts we just went through -- that venue is proper in

the District of Massachusetts.

Unlike all of the other elements that we talked about -- remember I said "proof beyond a reasonable doubt" numerous times -- but unlike all the elements that I previously described, the government has to prove venue by a preponderance of the evidence. That's a legal term, "preponderance of the evidence." That means, to establish venue by a preponderance of the evidence, the government must prove that the fact is more likely true than not true, more likely true than not true.

02:12 To establish venue in this district, the government need not prove that the crimes themselves were committed entirely in this district, or that the defendant himself was present here.

I'm now going to focus you on conspiracy.

With regard to the conspiracy charged in Count One, there's no requirement that the entire conspiracy took place here in Massachusetts, or that the agreement was formed here. But for you to return a guilty verdict on the conspiracy charge in Count One, the government must prove by a preponderance of

02:12 the evidence that any overt act in furtherance of the agreement took place here in Massachusetts.

Alternatively -- now, I just want you to focus only on the conspiracy count with respect to what I'm about to tell you. Alternatively, with respect to the conspiracy count only, the government has this alternative theory of venue. Under

federal law, where an offense is begun or committed outside the jurisdiction of any particular state or district, venue for prosecution of the offense is established in the district where the defendant is arrested or is first brought. For venue to be established for the conspiracy count under this alternative theory, the government must prove that it is more likely true than not true that the offense was begun or committed outside of the United States, and that the defendant was first brought to the District of Massachusetts. The government must also
02:13 prove that the essential conduct elements of the conspiracy took place outside of the United States.

If the government fails to prove venue by a preponderance of the evidence with respect to any count, you must find the defendant not guilty of that count only. So for every single one of these verdict slips, you also have to find not only that the government proved the elements beyond a reasonable doubt, but also that it proved venue by a preponderance of the evidence, more likely true than not true.

I am now at the end of the middle section of this
02:14 charge. The hard part has been completed, and now I want to talk to you about the mechanics of deliberation.

Okay, so let me talk to you about going back into that jury room. The first thing that you should do upon going to the jury room is to choose a foreperson. When I was a brand-new young judge, which I no longer am, I used to look at you

> assist in the commission of the offense or the proceeds of such offense or property derived therefrom.

18 U.S.C. § 1029(h).

The Act also amended section 1030(e)(2)(B) to specifically include a computer that "is used in interstate or foreign commerce, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B). Even prior to the 2001 amendment, however, at least one court held that the plain language of 18 U.S.C. § 1030 was a clear manifestation of congressional intent to apply that section extraterritorially. *See United States v. Ivanov*, 175 F. Supp. 2d 367, 374-75 (D. Conn. 2001).

Extraterritorial jurisdiction may exist not only based on specific Congressional intent, but also based on intended and actual detrimental effects within the United States. "The intent to cause effects within the United States . . . makes it reasonable to apply to persons outside United States territory a statute which is not extraterritorial in scope." *United States v. Muench*, 694 F.2d 28, 33 (2d Cir. 1982). "It has long been a commonplace of criminal liability that a person may be charged in the place where the evil results, though he is beyond the jurisdiction when he starts the train of events of which that evil is the fruit." *United States v. Steinberg*, 62 F.2d 77, 78 (2d Cir. 1932).

Other sources of extraterritorial jurisdiction may include 18 U.S.C. § 7, which defines the special maritime and territorial jurisdiction of the United States, and 18 U.S.C. §§ 3261-3267, which govern criminal offenses committed outside of the United States by members of the military and persons employed by or accompanying them.

B. Venue

1. Background

A combination of constitutional provisions, statutes, and rules govern venue. *See* 2 Charles Alan Wright, *Federal Practice & Procedure* § 301 (3d ed. 2000). The Constitution mandates that the defendant be tried in the state and district where the crime was committed. *See* U.S. Const. art. III, § 2, cl. 3; U.S. Const. amend. VI. This principle is implemented by Federal Rule of Criminal Procedure 18, which states in full: "Unless a statute or these rules permit otherwise, the government must prosecute an offense in a district where

the offense was committed. The court must set the place of trial within the district with due regard for the convenience of the defendant and the witnesses, and the prompt administration of justice." Fed. R. Crim. P. 18. However, the Constitution and Rule 18 still leave questions unanswered in many network crime cases, such as how to define where an offense has been "committed" or how to deal with crimes committed in multiple states or countries.

Note that when a defendant is charged with more than one count, venue must be proper with respect to each count. *See United States v. Salinas*, 373 F.3d 161, 164 (1st Cir. 2004) ("The criminal law does not recognize the concept of supplemental venue."). If no single district has proper venue for all potential counts, prosecutors can either charge the defendant in multiple districts and seek transfer to a single district or bring all charges in one district and seek a waiver from the defendant. Rule 20 of the Federal Rules of Criminal Procedure allows transfer of prosecution for purposes of entering a guilty plea from the district where the indictment is pending to the district where the defendant is arrested, held, or present. Similarly, Rule 21 allows a court to transfer a prosecution for trial, upon the defendant's motion, to another district for the convenience of the parties and witnesses. Note, however, that both rules require the explicit consent and cooperation of the defendant. A defendant may also waive any objections to improper venue, either explicitly or by failing to object when the defect in venue is clear. *See United States v. Roberts*, 308 F.3d 1147, 1151-52 (11th Cir. 2002); *United States v. Novak*, 443 F.3d 150, 161 (2d Cir. 2006).

2. Locations of Network Crimes

Applying the principles of venue to network crimes is not always a straightforward endeavor. As described above, the central inquiry in venue analysis is determining where the crime was committed. Yet, "in today's wired world of telecommunication and technology, it is often difficult to determine exactly where a crime was committed, since different elements may be widely scattered in both time and space, and those elements may not coincide with the accused's actual presence." *United States v. Saavedra*, 223 F.3d 85, 86 (2d Cir. 2000); *see United States v. Rowe*, 414 F.3d 271 (2d Cir. 2005) (finding venue in district where agent connected to Internet, entered chat room, and saw defendant's posting in child porn case); *United States v. Allamon*, 2005 WL 2542905 (S.D.N.Y. 2005) (finding venue in district where victims viewed website used in fraudulent scheme).

None of the intrusion crimes discussed in Chapter 1 contains a specific venue provisions. Moreover, few reported cases address venue for these crimes. *See, e.g., United States v. Ryan*, 894 F.2d 355 (10th Cir. 2000) (noting that 18 U.S.C. § 1029 does not specify venue); *Berger v. King World Productions, Inc.*, 732 F. Supp. 766 (E.D. Mich. 1990) (examining venue under 28 U.S.C. § 1391(b) in a civil suit arising pursuant to 18 U.S.C. § 2511).

Multidistrict offenses "may be . . . prosecuted in any district in which such offense was begun, continued, or completed." 18 U.S.C. § 3237(a). Note that only the "essential conduct elements" of a crime qualify. *United States v. Rodriguez-Moreno*, 526 U.S. 275, 280 (1999). For instance, section 1030(a)(2)(C) prohibits intentionally accessing a computer without or in excess of authorization, and thereby obtaining information from any protected computer. The two essential conduct elements in section 1030(a)(2)(C) are "accessing" a computer and "obtaining" information. Thus, it would seem logical that a crime under section 1030(a)(2)(C) is committed where the offender initiates access *and* where the information is obtained.

The exact location of each event—the "accessing" and the "obtaining"—may not always be easily determined.

> Example: *An intruder located in California uses communications that pass through a router in Arizona to break into a network in Illinois and then uses those network connections to obtain information from a server in Kentucky.*

The intruder initiated access in California, and the router in Arizona enabled that access. Arguably, however, the intruder did not achieve access until reaching the network in Illinois. Of course, one could also argue that access did not occur until the intruder reached the server in Kentucky where the information was located. Likewise, one could argue that the intruder obtained the information in Kentucky, or that he did not obtain the information until it reached him in the district where he was located, in this case, California.

This example illustrates an offense governed by 18 U.S.C. § 3237(a). Under any of the options discussed above, the appropriate venue would seem to include both of the endpoints—that is, the district in which the offender is located (California) and the district in which the information is located (Kentucky). It is likely that venue is also proper at some, if not all, of the points in between, since venue may lie "in any district in which [a continuing] offense was begun, continued, or completed." 18 U.S.C. § 3237(a). Under this

section, the "accessing" and "obtaining" arguably continued in Arizona and Illinois. Certainly, venue seems proper in Illinois where the intruder broke into the network. Whether the intruder committed a crime in Arizona is less clear.

Prosecutors looking to fix venue in the locale through which communications passed, as in the case of the router in Arizona, should look closely at the facts to determine whether venue in that district would satisfy the framework discussed above. The case for "pass through" venue may be stronger where transmission of the communications themselves constitutes the criminal offense (e.g., when a threatening email is sent in violation of 18 U.S.C. § 1030(a)(7)) and the path of transmission is certain (e.g., when an employee's email is sent through a company mail server in a particular state). *See, e.g.*, *United States v. Brown*, 293 Fed. Appx. 826 (2d Cir. 2008) (venue for wire fraud charges appropriate in district through which wire transfer related to fraudulent scheme passed, even though transfer was not processed in that district); *United States v. Offill*, 2009 WL 1649777 (E.D. Va. 2009) (spam emails related to fraudulent scheme passed through server located in district cited as one factor in favor of retaining venue in that district). By contrast, in cases where the path of transmission is unpredictable, a court may find it difficult to conclude that a crime was committed in a district merely because packets of information happened to travel through that district. *Cf. Ashcroft v. ACLU*, 535 U.S. 564, 602 (2002) (Kennedy, J., concurring) ("In the context of COPA, it seems likely that venue would be proper where the material originates or where it is viewed. Whether it may be said that a website moves 'through' other venues in between is less certain."). Of course, where the "pass through" computer itself is attacked, venue would likely be proper based on the attack, without reference to pass-through rationale.

Federal prosecutors should also take note of the Department of Justice's policies for wire and mail fraud, which may be analogous. For wire fraud, section 967 of the Department's Criminal Resource Manual provides that prosecutions "may be instituted in any district in which an interstate or foreign transmission was issued or terminated." Crim. Resource Manual § 967. Although the text of section 967 refers only to the place of issuance or termination, the case cited in support of that proposition, *United States v. Goldberg*, 830 F.2d 459, 465 (3d Cir. 1987), relies on 18 U.S.C. § 3237(a), which also includes the place where the conduct continued, thus leaving open the door to "pass through" venue. In the case of mail fraud, section 9-43.300 of the U.S. Attorneys' Manual states that Department of Justice policy "opposes mail fraud venue based solely

on the mail matter passing through a jurisdiction." USAM 9-43.300; *see also* Crim. Resource Manual § 966.

In some cases, venue might also lie in the district where the effects of the crime are felt. The Supreme Court has not faced that question directly. *See United States v. Rodriguez-Moreno*, 526 U.S. 275, 279 n.2 (1999) ("The Government argues that venue also may permissibly be based upon the effects of a defendant's conduct in a district other than the one in which the defendant performs the acts constituting the offense. Because this case only concerns the *locus delicti*, we express no opinion as to whether the Government's assertion is correct."). However, other courts that have examined the issue have concluded that venue may lie "where the effects of the defendant's conduct are felt, but only when Congress has defined the essential conduct elements in terms of those effects." *United States v. Bowens*, 224 F.3d 302, 314 (4th Cir. 2000), *cert. denied,* 532 U.S. 944 (2001); *see also United States v. Krangle*, 142 Fed. Appx. 504, 505 (2d Cir. 2005) (upholding venue in district where continuing offense had "significant effects"). Thus, charges under provisions like 18 U.S.C. § 1030(a)(5) may be brought where the effects are felt because those charges are defined in terms of "loss," even if the bulk of network crimes may not be prosecuted in a district simply because the effects of the crime are felt there. Prosecutors seeking to establish venue by this method are encouraged to contact CCIPS at (202) 514-1026.

C. Statute of Limitations

For criminal prosecutions, the Computer Fraud and Abuse Act subsections discussed in Chapter 1 do not contain a specific statute of limitations. Civil actions have a two-year statute of limitations. *See* 18 U.S.C. § 1030(g) (requiring *civil* actions to be brought "within 2 years of the date of the act complained of or the date of the discovery of the damage"); *see also* 18 U.S.C. § 2707(f) (creating two-year statute of limitations for *civil* actions); 18 U.S.C. § 2520(e) (providing that any *civil* action "may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation").

In the absence of a specific statute of limitations, the default federal limitations period of five years applies. *See* 18 U.S.C. § 3282. There are two exceptions to this five-year default limit: 18 U.S.C. §§ 1030(a)(1) and (a)(5)(A) (if the violation causes the type of damage identified in section 1030(c)(4)

United States Court of Appeals
For the First Circuit

No. 23-1779

UNITED STATES,

Appellee,

v.

VLADISLAV KLYUSHIN, a/k/a John Doe 1, a/k/a Vladislav Kliushin,

Defendant - Appellant.

APPELLEE'S BRIEFING NOTICE

Issued: March 29, 2024

Appellee's brief must be filed by **April 24, 2024**.

The deadline for filing appellant's reply brief will run from service of appellee's brief in accordance with Fed. R. App. P. 31 and 1st Cir. R. 31.0. Parties are advised that extensions of time are not normally allowed without timely motion for good cause shown.

Presently, it appears that this case may be ready for argument or submission at the coming **July/August, 2024** session.

The First Circuit Rulebook, which contains the Federal Rules of Appellate Procedure, First Circuit Local Rules and First Circuit Internal Operating Procedures, is available on the court's website at www.ca1.uscourts.gov. Please note that the court's website also contains tips on filing briefs, including a checklist of what your brief must contain.

Failure to file a timely brief in compliance with the federal and local rules could result in the appellee not being heard at oral argument. See 1st Cir. R. 45.0.

Maria R. Hamilton, Clerk

UNITED STATES COURT OF APPEALS
FOR THE FIRST CIRCUIT
John Joseph Moakley
United States Courthouse
1 Courthouse Way, Suite 2500
Boston, MA 02210
Case Manager: Gloria - (617) 748-4214

cc:
Karen Lisa Eisenstadt
Marc Fernich
Stephen Emanuel Frank
Carol Elisabeth Head
Seth B. Kosto
Donald Campbell Lockhart
Maksim Nemtsev